JAPAN PATENT OFFICE

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 4, 2001

Application Number: Patent Application No. 2001-308387

Applicant(s): FUJITSU LIMITED

October 26, 2001

Commissioner,
Japan Patent Office Kozo OIKAWA

Certificate No. 2001-3093372

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年１０月 ４日

出願番号
Application Number: 特願２００１－３０８３８７

出願人
Applicant(s): 富士通株式会社

２００１年１０月２６日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号 出証特２００１－３０９３３７２

【書類名】　特許願

【整理番号】　0151680

【提出日】　平成13年10月 4日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 13/00

【発明の名称】　パケット中継処理装置

【請求項の数】　20

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　嶋田　邦昭

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　横山　乾

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　栗田　敏彦

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　勝山　恒男

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　川崎　健

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通

株式会社内

【氏名】　高場　浩一

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　▲蔭▼山　博靖

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100074099

【住所又は居所】　東京都千代田区二番町８番地２０　二番町ビル３Ｆ

【弁理士】

【氏名又は名称】　大菅　義之

【電話番号】　03-3238-0031

【選任した代理人】

【識別番号】　100067987

【住所又は居所】　神奈川県横浜市鶴見区北寺尾７－２５－２８－５０３

【弁理士】

【氏名又は名称】　久木元　彰

【電話番号】　045-573-3683

【先の出願に基づく優先権主張】

【出願番号】　特願2001- 90122

【出願日】　平成13年 3月27日

【手数料の表示】

【予納台帳番号】　012542

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9705047

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　パケット中継処理装置

【特許請求の範囲】

【請求項１】　ネットワーク接続装置を有するパケット中継処理装置であって、

上記ネットワーク接続装置がセッションを管理するセッション管理部と、

上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている

ことを特徴とするパケット中継処理装置。

【請求項２】　上記ネットワーク接続装置は、更に、上記パケットのルーティング先に関するルーティング情報を格納するルーティングテーブルと、

上記セッションの開始時に、上記ルーティング情報に基づいて上記パケットのルーティング先を決定するルーティング処理部を更に備え、

上記パケット処理部は、上記パケットを決定された上記ルーティング先に出力する、

ことを特徴とする請求項１に記載のパケット中継処理装置。

【請求項３】　上記パケット中継処理装置は、更に、サーバを備え、

上記サーバは、上記ルーティングテーブルに上記ルーティング情報を書き込むネットワーク制御部を備える、

ことを特徴とする請求項２に記載のパケット中継処理装置。

【請求項４】　上記パケット中継処理装置は、さらに、サーバを備え、

上記サーバは、上記セッションを管理する外部セッション管理部を備え、

上記セッション管理部は、与えられた条件に応じて上記セッションに関するセッション情報を上記サーバに転送し、

上記外部セッション管理部は、受信した上記セッション情報に基づいて上記セッションを管理する、

ことを特徴とする請求項１に記載のパケット中継処理装置。

【請求項５】　上記ネットワーク接続装置は、更に処理振分部と複数のサービス処理部を備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも１つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする請求項１に記載のパケット中継処理装置。

【請求項６】　上記パケット中継処理装置は、更にサーバを備え、

上記サーバは、外部サービス処理部を備え、

上記処理振分部は、与えられた条件によって、上記パケットを上記サーバに転送し、

上記外部サービス処理部は、受信したパケットに対するサービスを実行する、

ことを特徴とする請求項５に記載のパケット中継処理装置。

【請求項７】　上記パケット中継処理装置は、サーバを更に備え、

上記サーバは、パケット詳細解析部を備え、

上記ネットワーク接続装置は、更に処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって上記パケットを上記パケット詳細解析部に転送し、

上記パケット詳細解析部は、上記パケットを解析することにより上記パケットに対するサービス内容を決定し、決定した上記サービス内容を上記ネットワーク接続装置に設定し、

上記設定後、上記ネットワーク接続装置は、上記決定されたサービス内容に基づいて上記パケットを処理する、

ことを特徴とする請求項１に記載のパケット中継処理装置。

【請求項８】　上記ネットワーク接続装置は、上記セッションに関するセッション情報を格納するセッションテーブルと、上記パケットに対するサービスを実行するための規則を記述するポリシーを格納するポリシーテーブルを備え、

上記セッション管理部は、上記パケットを受信した場合、上記パケットに含まれる情報を検索キーとして用いてセッションテーブルを検索し、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されていない場合には、上記セッション管理部は、さらに上記パケットに含まれる

情報を検索キーに基づいて、上記ポリシーテーブルから上記ポリシーを取得し、上記取得したポリシーに基づいて、上記セッション情報を上記セッションテーブルに書き込み、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されている場合には、上記セッション管理部は、上記セッションの状態に基づいて、上記セッションテーブルに格納されたセッション情報を管理することを特徴とする請求項５又は請求項６に記載のパケット中継処理装置。

【請求項９】　上記パケット中継処理装置はサーバを備え、

上記サーバは、上記ポリシーを上記ポリシーテーブルに書き込むサービス制御部を備える、

ことを特徴とする請求項８に記載のパケット中継処理装置。

【請求項１０】　上記セッション管理部は、更に、上記セッションが終了してから所定時間経過した後に、上記終了したセッションに関するセッション情報を上記セッションテーブルから削除することを特徴とする請求項１乃至請求項９いずれか１項に記載のパケット中継処理装置。

【請求項１１】　上記ネットワーク接続装置は、更に、パケットに関する統計情報を取得するためのカウンタを備えることを特徴とする請求項１乃至請求項１０のいずれか１項に記載のパケット中継処理装置。

【請求項１２】　複数のポリシーは複数のグループに分けられ、

上記ネットワーク接続装置は、更に、上記グループ毎に各ポリシーが有効であるか否かを設定することを特徴とする請求項８又は請求項９に記載のパケット中継処理装置。

【請求項１３】　上記ネットワーク接続装置は、更に、上記パケットのログを採取するために、上記パケットの少なくとも一部を上記サーバに転送することを特徴とする請求項９に記載のパケット中継処理装置。

【請求項１４】　上記セッション情報は、上記サーバに上記パケットを転送するべきか否かを示すサーバ転送指示情報を含み、上記処理振分部は、上記サーバ転送指示情報に基づいて、上記パケットを上記サーバへの転送を行うか否かを決定する事を特徴とする請求項９に記載のパケット中継処理装置。

【請求項１５】　上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがＨＴＴＰプロトコルのＧＥＴパケットである場合、上記パケットに含まれるＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする請求項７に記載のパケット中継処理装置。

【請求項１６】　上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがＦＴＰプロトコルのＰＯＲＴ命令、或いはＰＡＳＶ命令のＡＣＫである場合、上記セッションのデータコネクションのＩＰアドレスとポート番号に基づいて、上記パケットに対するサービスを決定する、
ことを特徴とする請求項７に記載のパケット中継処理装置。

【請求項１７】　上記パケット詳細解析部は、上記サーバの負荷を分散させる処理を行う場合、上記負荷の振分先となる振分先サーバが決定されるまで、上記振分先サーバに代わって応答することを特徴とする請求項７に記載のパケット中継処理装置。

【請求項１８】　上記パケット詳細解析部は、上記パケットを解析することにより、上記セッションテーブルに、上記パケットに対するサービスの種類、変換用ＩＰアドレス及びポート番号、シーケンス番号及びＡＣＫ番号差分を書き込む、
ことを特徴とする請求項７に記載のパケット中継処理装置。

【請求項１９】　パケット中継処理装置におけるネットワーク接続装置であって、
上記ネットワーク接続装置がセッションを管理するセッション管理部と、
上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている
ことを特徴とするネットワーク接続装置。

【請求項２０】　パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムであって、
セッションを管理し、
上記セッション管理に基づいて上記パケットを中継する

ことを含む処理を上記コンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、サーバ負荷分散制御、ＮＡＴ（Network Address Translation）、帯域制御、ＶＰＮ（Virtual Private Network）、ファイアウォールサービス機能を持ったサーバを最適化するためのパケット中継処理装置に関する。

【０００２】

【従来の技術】

現在、WWW（World WideWeb）やＥ－ｍａｉｌ、携帯電話におけるパケット通信サービスの普及により、インターネットが急速に大規模化している。それに伴い、ネットワークのさらなる高速化や、セキュリティ等の高機能化の要求が高まって来ている。現状のネットワークサービスの実行形態は、サーバと、ＮＩＣ（NetworkInterface Card）等のネットワーク接続装置という構成が一般的である。昨今のネットワークサービスは複雑化してきており、様々な、そして新しい要求に対し柔軟に対応できるという点で、サーバというプラットホームが適している。

【０００３】

図３９に従来のパケット中継処理装置の構成を示す。同図はサーバとネットワーク接続装置がネットワーク上で、サービスを実現する一般的な構成を示しており、矢印は制御情報の流れ、太い矢印はパケット情報を示す。

【０００４】

同図において、１００はサーバであり、パケット処理部１０１と、サービス１処理部～サービスｎ処理部１０２と、サービス１制御部～サービスｎ制御部１０３を備える。

【０００５】

サービス１処理部～サービスｎ処理部１０２は、サービス１制御部～サービスｎ制御部１０３で定めるポリシーに従い、セッション管理やルーティングを行う

とともに、フィルタリングや負荷分散等のサービス処理を行う。

【０００６】

１０４はネットワーク接続装置であり、ネットワーク接続部を介してネットワークから入力されたパケットは、ネットワーク接続装置１０４、パケット通信部１０５を介してサーバ１００のパケット処理部１０１に送られ、パケットが処理される。

【０００７】

【発明が解決しようとする課題】

最近の急激なインターネットの大規模化のため、ネットワークを流れるパケットの量は指数関数的な伸びを示している。このため、従来のサーバでは、要求される処理速度に応えきれなくなってきており、サーバを高速化する技術が求められている。また、新しいプラットホームを作る上で、サーバの多くのサービスを統合することができるという点は、できる限り損なわないようにしたい。

【０００８】

本発明は上記問題を解決するためになされたものであって、多くのネットワークワービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化することを目的とする。

【０００９】

【課題を解決するための手段】

図１は本発明の概要を説明する図である。同図において、１はサーバ、２はネットワーク接続装置である。本発明においては、ネットワーク接続装置を統合し、従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置２上に配置してパケット中継処理部を構成し、該パケット中継処理部により、ネットワーク接続装置２上でセッション管理に基づくパケット中継処理を行う。

【００１０】

また、ネットワーク接続装置２上に、処理振分部２ｃと複数のサービス処理部２ｄを設け、サーバ１により設定されるポリシーに従って、処理振分部２ｃにより、複数のサービス処理部２ｄへのセッション管理に基づく振り分けを行う。

【００１１】

さらに、サーバ１に外部セッション管理機能を設け、セッション数がネットワーク接続装置２のセッションテーブル登録数を上回った場合等に、サーバ１によりセッション管理を行うようにすることもできる。

【００１２】

また、サーバ１に外部サービス処理部を設け、上記処理振分部２ｃが、パケットを上記サーバ１に転送し、サーバ１の外部サービス処理部でサービス処理を実行させるようにしたり、サーバ１にパケット詳細解析部を設け、サーバ１がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置２に設定し、ネットワーク接続装置２は、以後同じセッションに対して上記決定されたサービス内容に基づき中継処理を行うようにすることもできる。

【００１３】

以上のように本発明においては、次のようにして前記課題を解決する。

（１）上記ネットワーク接続装置２に、パケット処理部２ａとセッション管理部２ｂからなる、セッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置２により、セッション管理に基づく中継処理を行う。

【００１４】

上記のように、従来サーバ上に配置していた機能をネットワーク接続装置２で行っているので、サーバ１のＣＰＵ使用率を下げることができる。また、ネットワーク接続装置２でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録しているので、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

（２）上記（１）において、パケット中継処理装置のサーバ１に外部セッション管理機能を設け、ネットワーク接続装置２が、与えられた条件に応じてセッション情報を上記サーバ１に転送し、サーバ１によりセッション管理を行う。

【００１５】

これにより、セッション数がネットワーク接続装置２のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置２で溢れた分をサーバ１で管理することができる。

（３）上記（１）において、ネットワーク接続装置２に処理振分部２ｃと複数のサービス処理部２ｄを設け、処理振分部２ｃが、上記複数のサービス処理部２ｄへのパケットの振分を行いサービス処理を実行させる。

【００１６】

上記のように、処理振分部２ｃと複数のサービス処理部２ｄをサーバ１より高速に処理できるネットワーク接続装置２に配置することにより、サーバ１のＣＰＵの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

（４）上記（３）において、サーバ１に外部サービス処理部を設け、処理振分部２ｃが、与えられた条件によって、パケットの振分を行いサーバ１の外部サービス処理部でサービス処理を実行させる。

【００１７】

上記のようにサービス処理を、ネットワーク接続装置２とサーバ１の両方で実行できるようにすることにより、ネットワーク接続装置２上で実現するのは困難なサービス処理をサーバ１で行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

（５）上記（１）において、ネットワーク接続装置２に振分処理部２ｃとサービス処理部２ｄを設け、また、サーバ１にパケット詳細解析部（不図示）を設け、処理振分部２ｃが、与えられた条件によってパケットをサーバ１に転送し、サーバ１がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置２に設定し、ネットワーク接続装置２は、以後同じセッションに対して上記設定されたサービス内容に基づき中継処理を行う。

【００１８】

上記のように、サーバ１においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置２に設定し、以後同じセッションに対してネットワーク接続装置２が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバ１で全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【００１９】

【発明の実施の形態】

図２は本発明の第１の実施例のパケット中継処理装置の構成を示す図である。

同図において、１１はサーバであり、ネットワーク制御部１２を備えており、ネットワーク制御部１２は、管理者が入力したルーティング情報を制御情報通信部３１を通して、ネットワーク接続装置２０のルーティングテーブル２３ａに書き込む。制御情報通信部３１は、例えばＰＣＩ（Peripheral Components Interconnect）バスやシリアルインターフエースである。

【００２０】

２０はネットワーク接続装置であり、本実施例のネットワーク接続装置２０は、図３９に示した複数のネットワーク接続装置１０４を統合したものであり、パケット処理部２１、セッション管理部２２、セッションテーブル２２ａ、ルーティング処理部２３、ルーティングテーブル２３ａを備え、前記図３８のサーバが行っていた、パケット処理、セッション管理、ルーティング処理等は、ネットワーク接続装置２０で行われる。

【００２１】

図２において、ネットワークから入力された図３に示すパケットは、ネットワーク接続部３０を通してネットワーク接続装置２０のパケット処理部２１に送られる。ネットワーク接続部３０は、例えばイーサネット（登録商標）コントローラである。

【００２２】

パケット処理部２１では、後述する図４のフローチャートに示す処理を行い、パケットをセッション管理部２２に送る。セッション管理部２２では、後述する図５のフローチャートに示すようにセッション管理を行い、パケットをパケット処理部２１に渡す。

【００２３】

パケット処理部２１は、後述する図４に示すようにパケットの処理を行い、パケットをネットワーク接続部３０を介して、ネットワークに出力する。

図４に上記パケット処理部の処理フローを示す。

【００２４】

同図に示すように、パケット処理部２１は、ネットワークから入力されたパケットのバッファリングを行い（ステップＳ１）、チェックサムのチェックを行う（ステップＳ２）。ついで、パケット処理部２１は、パケットのデフラグメンテーションを行い（ステップＳ３）、パケットをセッション管理部２２へ送る（ステップＳ４）。

【００２５】

そして、パケット処理部２１は、セッション管理部２２から送られてくるパケットのフラグメンテーション（ステップＳ５）、チェックサム再計算を行い（ステップＳ６）、パケットをネットワークに出力する。なお、パケット処理部２１における処理は従来のパケット処理部における処理と同じである。

【００２６】

図５に上記セッション管理部２２の処理フローを示す。

同図に示すように、セッション管理部２２にパケットが送られてくると、セッション管理部２２では、そのパケットに対応するセッションデータをセッションテーブル２２ａから検索する（ステップＳ１１）。セッションテーブル２２ａは、セッションを管理するためのセッションデータを格納するテーブルである。図６にセッションテーブル２２ａの構成例を示す。図６に示すように、セッションデータは、セッションを識別するセッションＩＤ（IDentifier）、セッションを一意に決定するためのセッション検索キー（宛先／送信元アドレス、宛先／送信元ポート、プロトコル）、セッションの状態、および出力先などを項目として持つ。

【００２７】

ステップＳ１１において、セッション管理部２２は、パケットのＩＰヘッダ内の送信元／宛先ＩＰアドレス、及びＴＣＰヘッダ内のプロトコル、送信元／宛先ポート等の情報をキーにしてセッションテーブル２２ａを検索する。

【００２８】

セッション管理部２２に送られてきたパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが、セッションテーブル２２ａに登録されていない場合には（ステップＳ１２：Ｎｏ）、その送られてきたパケットは、あ

るセッションの最初のパケットであるので、セッション管理部２２は、セッションテーブル２２ａにそのセッションに関するセッションデータを登録する（ステップＳ１３）。すなわち、ステップＳ１３において、セッション管理部２２は、送られてきたパケットのヘッダ内の情報に基づいて、図６に示すセッションテーブル２２ａにセッション検索キー（宛先／送信元アドレス、宛先／送信元ポート、プロトコル）や、セッションの状態を書き込む。

【００２９】

ついで、ルーティング処理部２３でルーティングテーブル２３ａの検索を行い、検索の結果として得られた出力先をセッションテーブル２２ａに書き込む（ステップＳ１４）。

【００３０】

一方、セッションテーブル２２ａにそのパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には（ステップＳ１２：Ｙｅｓ）、セッション管理部２２は、そのセッションの状態を検査して、状態が遷移するかどうかを判定する（ステップＳ１５）。そして、状態が遷移する場合には（ステップＳ１５：Ｙｅｓ）、セッション管理部２２は、セッションテーブル２２ａ内のセッション状態を書き換える（ステップＳ１６）。

【００３１】

そして、セッション管理部２２は、セッションの状態遷移が終わりセッションクローズの場合、すなわちセッション状態がＴＩＭＥ＿ＷＡＩＴ及びＣＬＯＳＥＤになっている場合には（ステップＳ１７：Ｙｅｓ）、そのセッションに関するセッション検索キー、セッション状態および出力先等をセッションテーブル２２ａのエントリから削除する（ステップＳ１８）。そして、処理が終わったパケットは出力先に送られる。セッションの状態がセッションクローズになっていない場合は（ステップＳ１７：Ｎｏ）、セッション管理部２２はステップＳ１８を行わず、処理が終わったパケットは出力先に送られる。

【００３２】

上記状態遷移は、ＴＣＰとその他のプロトコルではその判断が異なる。以下、ＴＣＰとその他のプロトコルを分けて説明する。

図７にＴＣＰの場合のセッション状態を示す。ＴＣＰの場合、セッション状態には図７に示すように、ＣＬＯＳＥＤ、ＳＹＮ＿ＲＥＣＶ、ＥＳＴＡＢ、ＦＩＮ＿ＲＥＣＶ、ＦＩＮ＿ＳＥＮＴ、ＴＩＭＥ＿ＷＡＩＴの６つの状態を設定する。

【００３３】

セッションテーブル２２ａのセッション状態には、図６に示すようにＣＬＯＳＥＤを除く上記５つの状態のうち、どの状態であるかが書き込まれている。

セッションが登録されていない時には状態がＣＬＯＳＥＤになっており、この状態でＳＹＮパケットが到着した場合、セッション状態はＳＹＮ＿ＲＥＣＶに状態遷移する。その際、セッション管理部２２は、セッションテーブル２２ａの「セッション状態」をＳＹＮ＿ＲＥＣＶに書き換える。ついで、セッション状態は、ＥＳＴＡＢ〈Ｅｓｔａｂｌｉｓｈｅｄ〉状態に遷移し、パケットが送受信される。そして、ＦＩＮパケットによりセッションは終了する。以下同様にして、ＳＹＮパケットとＦＩＮパケットの到着を検知することにより、セッション管理部２２は、セッションの開始と終了を検知することができる。

【００３４】

図８にＴＣＰの場合のセッション開始からセッション終了までの状態遷移の様子の一例を示す。

同図に示すように、クライアントとサーバ間で通信を行う場合、まずクライアントからＳＹＮパケットを送信する。ついで、サーバからＳＹＮ＿ＡＣＫパケットを返し、これに応答してクライアントからサーバにＡＣＫパケットを送信する。これにより、セッション状態は、ＳＹＮ状態からＥＳＴＡＢ（Ｅｓｔａｂｌｉｓｈｅｄ）状態に遷移し、以後、クライアントとサーバは、相互にパケットを送受信する。そして、セッションを終了する際、例えばクライアントからＦＩＮパケットをサーバに送信し、サーバがＦＩＮ＿ＡＣＫパケットをクライアントに送信し、これに応答してクライアントからＡＣＫパケットをサーバに送信することによりセッションが終了する（ＣＬＯＳＥＤ状態となる）。

【００３５】

これに対し、ＴＣＰ以外では、パケットにＳＹＮやＦＩＮのフラグが存在しない。図９に一例としてＵＤＰの場合の状態遷移を示す。図９に示すようにセッシ

ョンテーブル２２ａに登録されていないセッションに属するパケットが届いた場合には、セッション管理部２２は、そのセッションの状態をＥＳＴＡＢとする。セッションの終了は検知することができないので、セッション管理部２２は、タイマーによって一定時間パケットの通過が無い場合にはそのセッションをセッションテーブル２２ａから削除することによって対応する。

【００３６】

以上説明したように、本実施例においては、ネットワーク接続装置２０にセッション管理に基づくパケット中継処理機能を設け、従来サーバ１１上に配置していた機能をネットワーク接続装置２０が果たすようにしたので、サーバ１１のＣＰＵの使用率を下げることができる。

【００３７】

また、ネットワーク接続装置２０にセッション管理部２２を設け、セッション開始時にセッションテーブル２２ａに出力先を登録しているので、セッションの途中でルーティングテーブル２３ａのエントリが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【００３８】

図１０は本発明の第２の実施例のパケット中継処理装置の構成を示す図である。本実施例は、前記図２に示した第１の実施例のパケット中継処理装置において、セッション情報をサーバ１１に転送するサーバ転送部２４、セッション情報の通信を行うセッション情報通信部３２、外部セッション管理部１３、外部セッションテーブル１３ａを設けたものである。そして、ネットワーク接続装置２０のセッションテーブル２２ａが一杯になったとき、サーバ１１に設けた外部セッション管理部１３によりセッション管理を行う。その他の動作は第１の実施例と同様である。

【００３９】

図１１に本実施例におけるセッション管理部、外部セッション管理部における処理フローを示す。

同図に示すように、セッション管理部２２にパケットが送られてくると、セッション管理部２２、外部セッション管理部１３では、パケットのヘッダに格納さ

れた情報を検索キーとしてセッションテーブル２２ａ、外部セッションテーブル１３ａを検索する（ステップＳ２１）。セッションテーブル２２ａ、１３ａは前記図６で説明したセッションを管理するための情報を格納したテーブルである。

【００４０】

セッション管理部２２に送られてきたパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータがセッションテーブル２２ａ及び外部セッションテーブル１３ａに登録されていない場合には（ステップＳ２２：Ｎｏ）、そのパケットは、あるセッションの最初のパケットであるので、まず、セッション管理部２２は、セッションテーブル２２ａが一杯かを調べる（ステップＳ２３）。

【００４１】

セッションテーブル２２ａが一杯でない場合には（ステップＳ２３：Ｎｏ）、セッション管理部２２は、前記したようにセッションテーブル２２ａにそのセッションのセッションデータの登録を行う（ステップＳ２４）。ついで、ルーティング処理部２３でルーティングテーブル２３ａの検索を行い、結果をセッションテーブル２２ａに出力先を書き込む（ステップＳ２５）。

【００４２】

また、セッションテーブル２２ａに、パケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には（ステップＳ２２：Ｙｅｓ）、セッション管理部２２はセッション状態を検査して、状態が遷移するかどうかを判定する（ステップＳ２６）。そして、状態が遷移する場合には（ステップＳ２６：Ｙｅｓ）、セッション管理部２２は、セッションテーブル２２ａに格納されたセッションデータのセッション状態を書き換える（ステップＳ２７）。

【００４３】

そして、セッションの状態遷移が終わった後、セッションクローズの場合には（ステップＳ２８：Ｙｅｓ）、セッション管理部２２は、セッションテーブル２２ａのエントリからそのセッションデータを削除する（ステップＳ２９）。処理が終わったパケットは出力先に送られる。

【００４４】

一方、セッションの最初のパケットを登録する際、セッションテーブル２２ａが一杯の場合には（ステップＳ２３：Ｙｅｓ）、サーバ１１の外部セッション管理部１３で上記と同様の処理を行う。

【００４５】

すなわち、前記ステップＳ２４およびステップＳ２５で説明したようにして、外部セッション管理部１３は、外部セッションテーブル１３ａにそのパケットのセッションのセッションデータを登録し（ステップＳ３０）、ルーティング処理部２３は、ルーティングテーブルの検索を行って、結果を外部セッションテーブル１３ａに出力先を書き込む（ステップＳ３１）。

【００４６】

また、外部セッションテーブル１３ａにそのパケットのヘッダ内の情報とセッション検索キーが一致するセッションデータが登録されている場合には（ステップＳ２２：Ｙｅｓ）、外部セッション管理部１３は、外部セッションテーブル１３ａのセッション状態を検査して、セッション状態が遷移するかどうかを判定する（ステップＳ２６）。状態が遷移する場合には、外部セッション管理部１３は、外部セッションテーブル１３ａの「セッション状態」を書き換える（ステップＳ２７）。そして、セッションの状態遷移が終わった後、セッションクローズの場合には（ステップＳ２８：Ｙｅｓ）、外部セッション管理部１３は、セッションテーブル１３ａのエントリからそのセッションデータを削除する（ステップＳ２９）。

【００４７】

以上のように、本実施例においては、ネットワーク接続装置２０にセッション管理に基づくパケット中継処理機能を設け、従来サーバ１１上に配置していた機能をネットワーク接続装置２０が果たすようにしたので、第１の実施例と同様、サーバ１１のＣＰＵの使用率を下げることができる。また、第１の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【００４８】

さらに、セッション数がネットワーク接続装置２０のセッションテーブルに登録できる数を上回った場合、サーバ１１に設けた外部セッション管理部１３でセッション管理を行っているので、ネットワーク接続装置２０で溢れた分をサーバ１１で管理することが可能となる。

【００４９】

なお、上記説明ではサーバ１１に外部セッション管理部１３を設けてサーバ１１でセッション管理を行っているが、サーバ１１に外部セッションテーブル１３ａのみを設け、セッション管理はネットワーク接続装置２０のセッション管理部２２で行い、セッションテーブル２２ａで溢れたセッションを上記外部セッションテーブル１３ａに登録するようにしてもよい。

【００５０】

図１２は本発明の第３の実施例のパケット中継処理装置の構成を示す図である。本実施例によれば、ネットワーク接続装置２０に処理振分部２６とサービス処理部２７とポリシーテーブル２５を設け、サーバ１１により設定されるポリシーに従って、ネットワーク接続装置２０がフィルタリング、負荷分散、ＮＡＴ等のサービス処理を実行する。

【００５１】

同図において、１１はサーバであり、サーバ１１はサービス制御部１４を備えており、サービス制御部１４は、制御情報通信部３１を通して、ネットワーク接続装置２０のポリシーテーブル２５にポリシーを書き込む。ここで、ポリシーとは、フィルタリング、負荷分散等のサービスを実行するためのルールである。例えば、フィルタリングの場合には、ポリシーに基づいて、ポリシー検索キーの範囲でパケットを廃棄するか通過させるかが設定される。負荷分散の場合には、ポリシーに基づいて、仮想（代表）ＩＰアドレス：ポート番号と、振分先全てのサーバのＩＰアドレス：ポート番号が設定される。ＮＡＴの場合には、ポリシーに基づいて、変換後ＩＰアドレス：ポート番号が設定される。

【００５２】

２０はネットワーク接続装置であり、本実施例のネットワーク接続装置２０は、第１の実施例と同様、パケット処理部２１、セッション管理部２２、セッショ

ンテーブル２２ａ’を備え、さらに、上記ポリシーテーブル２５、処理振分部２６及び複数のサービス処理部２７を備える。サービス処理部２７は、パケットに適用されるサービスのタイプに応じて複数備えられる。

【００５３】

本実施例によれば、セッション管理部２２は、パケットを受信した場合、受信したパケットのヘッダ内の情報を用いて、セッションテーブル２２ａ’からセッションデータを検索する。そして、そのパケットのヘッダ内の情報が示すセッションデータがセッションテーブル２２ａ’に登録されている場合、上記とほぼ同様な処理が行われる。

【００５４】

一方、そのパケットのヘッダ内の情報によって示されるセッションデータがセッションテーブル２２ａ’に登録されていない場合、セッション管理部２２は、ポリシーテーブル２５を参照し、そのパケットに適用されるべきポリシーに基づいて、セッションデータを作成し、作成したセッションデータをセッションテーブル２２ａ’に格納する。

【００５５】

処理振分部２６は、パケットに対する適用サービスをセッションテーブル２２ａ’に格納されたセッションデータに基づいて判別し、判別された適用サービスに対応するサービス処理部２７に処理を振り分ける。複数のサービス処理部２７は、各サービスに必要な処理を行う。

【００５６】

以下、図１３及び図１４を用いて、本実施例に係わるセッションテーブル２２ａ’及びポリシーテーブル２５について説明する。図１３に、本実施例に係わるセッションテーブル２２ａ’の構造例を示す。セッションテーブル２２ａ’は、前記したようにセッションを管理するセッションデータを格納するテーブルである。セッションデータは、セッションＩＤ、セッション検索キー（宛先／送信元アドレスおよびポート、プロトコル等）や、セッションの状態、および出力先等を項目として含む。本実施例においては、図１３に示すように、セッションデータは、上記情報に加えて、さらに、適用サービスタイプ（フィルタリングや負荷

分散など）、そのサービス固有情報（振分先アドレスなど）、一貫性保持時間、イベントフラグ等を項目として含む。適用サービスタイプは、パケットに適用するべきサービスを示す。サービス固有情報は、適用するべきサービスに固有な情報を示す。例えば、適用サービスタイプが負荷分散である場合、サービス固有情報として振分先のアドレスが考えられる。一貫性保持時間は、セッションが終了してからセッションデータを保持すべき時間を示す。つまり、一貫性保持時間が経過するまで、セッションが終了してもセッションデータはセッションテーブル２２ａ’から削除されない。イベントフラグは、そのパケットまたはパケットのヘッダのログを採取するべきか否かを示す。イベントフラグが「オン」である場合、そのパケットまたはパケットのヘッダは、サーバに転送され、サーバによってログが採取される。

【００５７】

図１４に、ポリシーテーブルの構成例を示す。ポリシーテーブルは、パケットに対してサービスを実行するためのルールであるポリシーを格納する。図１４に示すようにポリシーは、ポリシーＩＤ、ポリシー検索キー、適用サービスタイプ、サービス固有情報、優先度、グループＩＤ、イベントフラグ、一貫性保持時間及びポリシーヒット数を含む。

【００５８】

ポリシーＩＤは、ポリシーを識別する情報である。ポリシー検索キーは、パケットに適用するべきポリシーを決定するための情報である。適用サービスタイプは、ポリシーに基づいてパケットに適用されるサービスを示す。サービス固有情報は、セッションデータと同様に、適用サービスに固有な情報を示す。優先度は、ポリシーの優先順位を示す数値である。優先度の値が低いほど、そのポリシーは優先される。優先度は、パケットのヘッダ内の情報が、複数のポリシーのポリシー検索キーに一致した場合、どのポリシーを優先すべきか決定する際に用いられる。グループＩＤは、ポリシーが属するグループを識別する情報である。イベントフラグ及び一貫性保持時間は、セッションデータと同様である。ポリシーヒット数は、そのポリシーに該当したセッションのカウント値を格納する。

【００５９】

イベントフラグ、一貫性保持時間、グループＩＤ及びポリシーヒット数を用いた処理についての説明は、各変形例の変形例として後述する。

以下、図１２に示す第３実施例にかかわるパケット中継処理装置の動作について図１５から図１９を用いて説明する。

【００６０】

まず、図１２に示すパケット中継処理装置において、ネットワークから入力されたパケットは、ネットワーク接続部３０を通り、パケット処理部２１に送られる。

【００６１】

パケット処理部２１は、前記した図４の処理フローに示したように、入力したパケットのバッファリングとチェックサムのチェック、デフラグメンテーションを行った後、そのパケットをセッション管理部２２へ送る。そして、パケット処理部２１は、セッション管理部２２から送られてきたパケットに対して、フラグメントとチェックサム再計算を行い、ネットワーク接続装置３０を介して、ネットワークに出力する。

【００６２】

本実施例のセッション管理部２２の処理フローを図１５に示す。

同図に示すように、パケットがセッション管理部２２に送られてくると、セッション管理部２２は、そのパケットのヘッダ内の情報を用いて図１３に示すセッションテーブル２２ａ’からセッションデータを検索する（ステップＳ４１）。

【００６３】

セッションテーブルの検索は、第１の実施例と同様、パケットのＩＰヘッダ内の送信元／宛先ＩＰアドレス、及びＴＣＰヘッダ内のプロトコル、送信元／宛先ポートの情報をキーにして行われる。

【００６４】

パケットのヘッダ内の情報とセッション検索キーが一致するセッションデータがセッションテーブル２２ａ’に登録されていない場合（ステップＳ４２：Ｎｏ）、セッションの最初のパケットであるので、セッション管理部２２は、そのセッションに対する適用サービスを判定するため、パケットのヘッダ内の情報を用

いて、図１４に示すポリシーテーブル２５からポリシーを検索する（ステップＳ４３）。

【００６５】

ポリシーテーブル２５は、ルーティング情報を持つとともに、サービスを適用する範囲を指定するポリシー検索キー（宛先／送信元アドレスおよびポート、プロトコル。任意や範囲指定でもよい）や適用サービスタイプ（フィルタリング廃棄や負荷分散など）、そのサービス固有の情報（全ての振り分け先アドレスなど）、および、優先度を持つ。

【００６６】

検索の結果、ポリシーテーブル２５のエントリとパケットのヘッダ内の情報がマッチした場合、そのポリシーをセッションテーブル２２ａ’の適用サービスタイプの欄に書き込む。つまり、セッション管理部２２は、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーをポリシーテーブル２５から取得する。続いて、セッション管理部２２は、パケットのヘッダ内の情報をセッション検索キーとするセッションデータを作成し、セッションテーブル２２ａ’に登録する。さらに、セッション管理部２２は、ポリシーに含まれる適用サービスタイプ及びサービス固有情報を、それぞれ登録したセッションデータの適用サービスタイプ欄及びサービス固有情報欄に書き込む（ステップＳ４４）。

【００６７】

ただし、複数のポリシーにマッチした場合には、ポリシーテーブル２５の優先度が高い順に処理する。また、同一サービスが複数マッチした場合には、優先度が最も高いものを採用し、残りを無効とする。

【００６８】

以下、ポリシーテーブル２５を検索した際、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーが複数存在した場合の処理について、より具体的に説明する。

【００６９】

まず、取得した複数のポリシーに含まれる適用サービスタイプが互いに競合しない場合、セッション管理部２２は、ポリシーの優先度の値が低い順に（つまり

、優先順位が高い順に）、複数の適用サービスタイプをセッションデータの適用サービスタイプの欄に書き込む。これにより、そのパケットは、優先順位が高い順に複数の適用サービスをうけることになる。

【００７０】

また、取得した複数のポリシーに含まれる適用サービスタイプが互いに競合する場合、セッション管理部２２は、複数のポリシーのうち、ポリシーの優先度の値が最も低いポリシーの適用サービスタイプのみをセッションデータの適用サービスタイプの欄に書き込む。これにより、そのパケットは、最も優先順位が高い適用サービスのみを受けることとなる。

【００７１】

以下、具体例を挙げて説明する。あるパケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーとして、以下の６ポリシーが取得されたとする。

ポリシー１：適用サービス＝フィルタ通過、優先度＝１０

ポリシー２：適用サービス＝フィルタ通過、優先度＝１００

ポリシー３：適用サービス＝フィルタ通過、優先度＝２００

ポリシー４：適用サービス＝負荷分散、優先度＝１０００

ポリシー５：適用サービス＝負荷分散、優先度＝２０００

ポリシー６：適用サービス＝負荷分散、優先度＝３０００

この場合、フィルタ通過と負荷分散は、互いに競合しない適用サービスタイプである。また、ポリシー１からポリシー３までの適用サービスタイプは全てフィルタ通過であるため、互いに競合する。同様に、ポリシー４からポリシー６までの適用サービスタイプは全て負荷分散であるため、互いに競合する。セッション管理部２２は、適用サービスタイプがフィルタ通過であるポリシーのうち、最も優先度の値が低いポリシー１及び、適用サービスタイプがフィルタ通過であるポリシーのうち、最も優先度の値が低いポリシー４を採用する。続いて、ポリシー１のフィルタ通過の優先度は、ポリシー４の負荷分散の優先度よりも低いため、セッション管理部２２は、セッションデータの適用サービスタイプの欄に、フィルタ通過を先にして、フィルタ通過及び負荷分散を書き込む。これにより、その

パケットは、フィルタ通過の後に負荷分散サービスを受けることになる。

【００７２】

ステップＳ４２でＹｅｓであった場合に行われるステップＳ４５からステップＳ４８までのセッション状態遷移に関する処理は、第１の実施例で説明したのと同様である。すなわち、セッションテーブル２２ａ’にセッションデータの登録がある場合には、セッション管理部２２は、セッションテーブル２２ａ’のセッション状態を検査して、状態が遷移するかどうかを判定する（ステップＳ４５）。そして、セッションの状態が遷移する場合には（ステップＳ４５：Ｙｅｓ）、セッション管理部２２は、セッションテーブル２２ａ’の状態を書き換える（ステップＳ４６）。そして、セッションの状態遷移が終わった後、セッション管理部２２は、そのセッションのセッションデータをセッションテーブル２２ａ’のエントリから削除する（ステップＳ４８）。処理が終わったパケットは、処理振分部２６に送られる（ステップＳ４９）。

【００７３】

処理振分部２６／サービス処理部２７の処理フローを図１６に示す。

処理振分部２６／サービス処理部２７では、パケットに対して適用サービスを判別し、各サービスに必要な処理を行う。

【００７４】

図１６において、パケットが処理振分部２６に入力されると、処理振分部２６は、そのパケットのヘッダ内の情報を用いてセッションテーブル２２ａ’から、入力したパケットに対応するセッションデータを検索する。検索の結果、得られたセッションデータで示される適用サービスタイプが、ルーティング処理である場合（ステップＳ５１）、処理振分部２６は、ルーティング処理を行うサービス処理部２７に処理を振り分ける。

【００７５】

入力パケットに対応するセッションテーブル２２ａ’に、ルーティング先が書き込まれていない場合、ポリシーテーブル２５のルーティングテーブル（不図示）を引き、出力先インターフェースと宛先ＭＡＣアドレスをセッションテーブル２２ａ’に書き込む。

【００７６】

より具体的に説明すると、処理振分部２６は、そのセッションデータにルーティング先が含まれているか否か判定する（ステップＳ５１）。セッションデータにルーティング先が含まれていない場合（ステップＳ５１：Ｙｅｓ）、処理を振り分けられたサービス処理部２７は、そのセッションデータに含まれる宛先ＩＰアドレスを用いてルーティングテーブル（図１２では不図示）を検索し、検索の結果得られた出力先インターフェースと宛先ＭＡＣアドレスをルーティング先として決定し（ステップＳ５２）、決定されたルーティング先をそのセッションデータに書き込む（ステップＳ５３）。以後、そのセッションデータに対応するセッションのパケットは、決定されたルーティング先に転送される。続いて、サービス処理部２７は、ステップＳ５６へ進む。

【００７７】

また、処理振分部２６が、セッションテーブル２２ａ’を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、負荷分散サービスを受けるべきパケットであり、且つ　セッションデータに振分先サーバが含まれていない、つまり、振分先サーバがまだ決定していないと判定した場合と判定した場合（ステップＳ５６：Ｙｅｓ）、処理振分部２６は、負荷分散処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７は、振分先サーバを決定し（ステップＳ５７）、決定された振分先のアドレスを対応するセッションテーブル２２ａ’のサービス固有情報欄に書き込み（ステップＳ５８）、ステップＳ６１に進む。

【００７８】

また、処理振分部２６が、セッションテーブル２２ａ’を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットがフィルタリング廃棄サービスを受けるべきパケットであると判定したならば（ステップＳ６１：Ｙｅｓ）、処理振分部２６は、パケット廃棄処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７は、そのパケットを廃棄し（ステップＳ６２）、処理を終了する。ステップＳ６１の判定でＮｏである場合、ステップＳ６３に進む。

【００７９】

処理振分部２６が、セッションテーブル２２ａ’を検索した結果得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、負荷分散もしくはＮＡＴサービスを実行するパケットならば、その入力パケットはヘッダ書換を受けるべきパケットであると判定する（ステップＳ６３：Ｙｅｓ）。処理振分部２６は、ヘッダ書換処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７は、そのパケットのＩＰヘッダとＴＣＰヘッダ上の送信元／宛先ＩＰアドレス、送信元／宛先ポート等を、セッションテーブル２２ａ’に格納されたセッションデータに従って書き換え、（ステップＳ６４）処理を終了する。なお、セッションデータに複数の適用サービスが格納されている場合、格納されている順に、入力パケットに該複数の適用サービスを実行する。

【００８０】

以上のように、本実施例においては、第１の実施例と同様、サーバ１１のＣＰＵの使用率を下げることができ、また、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【００８１】

さらに、処理振分部２６と複数のサービスに対応した複数のサービス処理部２７を、サーバ１１より高速に処理できるネットワーク接続装置２０に配置したので、サーバのＣＰＵの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

【００８２】

さらに、また、本実施例によれば、サービスに応じて複数のサービス処理部２７をネットワーク接続装置２０に備えることとしている。これにより、新たなサービスが必要になった場合、必要となったサービスに対応する新たなサービス処理部２７をネットワーク接続装置２０に追加することにより、容易に対応することが可能な柔軟な構成を実現する。例えば、新たに、ＶＰＮ（Virtual Private Network）暗号化サービスや復号化サービスが必要になった場合、新たに、ＶＰＮ暗号化サービスを行うサービス処理部２７及び復号化サービスを行うサービス

処理部２７を追加することにより対応することが可能である。

【００８３】

以下、図１７を用いて、より詳しくヘッダ書換処理について説明する。図１７に、本実施例においてネットワーク接続装置２０が負荷分散サービスを行う場合のパケットフローを示す。なお、図１７に示すパケットフローは、図１３に示すセッションテーブル２２ａ’内のセッションＩＤが２及び３であるセッションデータに対応している。また、矢印の方向は、パケットの送信される方向を示す。

【００８４】

アドレスが10.25.1.230 であるクライアントからアドレスが192.168.100.75であるサーバへパケットが送信される場合、まず、矢印Ａ１に示すように、クライアントからネットワーク接続装置２０へ「宛先アドレス：192.168.100.75、送信元アドレス：10.25.1.230」をヘッダに格納したパケットＰ１が送信される。ネットワーク接続装置２０のセッション管理部２２は、パケットＰ１に含まれる送信元アドレス10.25.1.230 及び宛先アドレス192.168.100.75等をキーとして図１３に示すセッションテーブル２２ａ’を参照し、セッションＩＤ＝３であるセッションデータを取得する。

【００８５】

取得されたセッションデータ内の適用サービスタイプは「ヘッダ書換」であるため、ネットワーク接続装置２０内の処理振分部２６は、ヘッダ書換処理を行うサービス処理部２７に処理を振り分ける。そのセッションデータ内の固有情報は「宛先アドレス：192.168.100.100 」であるため、処理を振り分けられたサービス処理部２７は、パケットＰ１内の宛先アドレスを「192.168.100.75」から「192.168.100.100」に書き換える。この結果、矢印Ａ２に示すように、ネットワーク接続装置２０からアドレスが192.168.100.100である振分先サーバへ「宛先アドレス：192.168.100.100、送信元アドレス：10.25.1.230」をヘッダに格納したパケットＰ２が送信される。

【００８６】

逆に、アドレスが192.168.100.100である振分先サーバからアドレスが10.25.1.230 であるクライアントへパケットが送信される場合、まず、矢印Ａ３に示す

ように、振分先サーバからネットワーク接続装置２０へ「宛先アドレス：10.25.1.230、送信元アドレス：192.168.100.100 」をヘッダに格納したパケットＰ３が送信される。ネットワーク接続装置２０のセッション管理部２２は、パケットＰ３に含まれる送信元アドレス及び宛先アドレスをキーとして図１３に示すセッションテーブル２２ａ’を参照し、セッションＩＤ＝２であるセッションデータを取得する。

【００８７】

取得されたセッションデータ内の適用サービスタイプ欄のエントリは「ヘッダ書換」であるため、ネットワーク接続装置２０内の処理振分部２６は、ヘッダ書換処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７は、そのセッションデータ内の固有情報に基づいて、パケット内の送信元アドレスを「192.168.100.100」から「192.168.100.75」に書き換える。この結果、矢印Ａ４に示すように、ネットワーク接続装置２０からアドレスが10.25.1.230であるクライアントへ「宛先アドレス：10.25.1.230、送信元アドレス：192.168.100.75」をヘッダに格納したパケットＰ４が送信される。このようにして、ネットワーク接続装置２０は、パケットのヘッダを書き換える事により、パケットの宛先サーバの負荷を分散させることができる。

【００８８】

図１８は本発明の第４の実施例のパケット中継処理装置の構成を示す図である。本実施例は、上記第３の実施例のパケット中継処理装置において、処理振分部２６にサーバ転送機能を設けるとともに、サーバ１１に外部サービス処理部１５を設け、サービス処理を、ネットワーク接続装置２０とサーバ１１の両方で実行できるようにしたものである。本実施例において、サービス処理をサーバ１１で実行する場合には、ポリシーテーブル２５にサービスの内容だけでなく、サーバ１１に転送することを設定しておく。その他の動作は第３の実施例と同様である。

【００８９】

図１８に示すように、外部サービス処理部１５は、第３実施例に係わるサービス処理部２７と同様に、適用サービスタイプに応じて複数の外部サービス処理部

１５をサーバ１１に備えられる。従って、第３実施例におけるサービス処理部２７と同様に、新たなサービスタイプが必要になった場合、新たなサービスタイプに対応する新たな外部サービス処理部１５をサーバ１１に追加することにより、容易に対応することが可能である。

【００９０】

本実施例にかかわるセッションテーブル２２ａ’及びポリシーテーブル２５の構成は、第３実施例とほぼ同様であるため、詳しい説明は省略する。異なる点は、第４実施例によれば、サービス処理部２７で行うサービスの内容に加えて、サーバ１１に転送して外部サービス処理部１５で行うサービスの内容をセッションテーブル２２ａ’及びポリシーテーブル２５に設定することができることである。

【００９１】

以下、本実施例の処理振分部２６、サービス処理部２７及び外部サービス処理部１５における処理の手順を図１９に示す。図１９において、ステップＳ５１からステップＳ６４までの処理は図１６と同じである。例えば、入力パケットに対応するセッションテーブル２２ａ’内のセッションデータで、適用サービスタイプが「ルーティング」が書き込まれ、且つ、ルーティング先が書き込まれていない場合、サービス処理部２７は、ポリシーテーブル２５のルーティングテーブルを引き、出力先インターフェースと宛先ＭＡＣアドレスをセッションテーブル２２ａ’内のセッションデータに書き込む。

【００９２】

このように、セッションテーブル２２ａ’の適用サービスタイプを参照し、適用サービスタイプにサーバ転送が設定されていない場合には、前記図１６で説明したように、適用サービスタイプに応じた処理を行い、ヘッダ書換えパケットの場合、ヘッダの書換処理を行う。

【００９３】

さらに、本実施例によれば、サービスの一部をサーバ１１内の外部サービス処理部１５が行う。そのために、処理振分部２６は、図１６のステップＳ５１からステップＳ６４の処理に加えて、以下の手順を行う。

【００９４】

すなわち、処理振分部２６は、セッションテーブル２２ａ’を検索して得られたセッションデータの適用サービスタイプ欄を参照し、入力パケットが、サーバ１１へ転送されるべきパケットであるか否かを判定する（ステップＳ７１）。セッションデータの適用サービスタイプ欄に「サーバ転送：ＯＮ」及び適用サービスタイプが設定されている場合には（ステップＳ７１：Ｙｅｓ）、処理振分部２６は、パケットに転送用ヘッダを付す処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７は、そのパケットに転送用ヘッダを付す。転送用ヘッダの内容は、例えば、適用サービスタイプ、そのパケットのセッションデータのセッションＩＤ及び入力インターフェースである。続いて、サービス処理部２７は、パケット通信部３３を介してパケットをサーバ１１の外部サービス処理部１５に転送する（ステップＳ７２）。適用サービスタイプに対応する外部サービス処理部１５は、受信したパケットを処理する（ステップＳ７３）。

【００９５】

外部サービス処理部１５の処理フローは前記した図１６と同様である。例えば、セッションデータ内でルーティング先が未決定の場合、外部サービス処理部１５は、ルーティング先を決定し、出力先インターフェースと宛先ＭＡＣアドレスをセッションテーブル２２ａ’に書き込む。

【００９６】

また、入力パケットが、負荷分散サービスをうけるべきパケットであり、セッションデータ内で振分先がまだ決定していない場合、外部サービス処理部１５は、振分先サーバを決定し、対応するセッションテーブル２２ａ’内のセッションデータのサービス固有情報欄に書き込む。入力パケットがフィルタリング廃棄サービスを受けるべきパケットならば、外部サービス処理部１５は、パケットを廃棄する。

【００９７】

そして、入力パケットが、負荷分散もしくはＮＡＴサービスを受けるべきパケットならば、外部サービス処理部１５は、そのパケットのＩＰヘッダとＴＣＰヘ

ッダ上の送信元／宛先ＩＰアドレス、送信元／宛先ポート等を、セッションテーブル２２ａ’内のセッションデータに従って書き換える。

【００９８】

なお、以上では、外部サービス処理部１５が、ネットワーク接続装置２０におけるサービス内容と同じサービスを行う場合について説明したが、外部サービス処理部１５で、例えば、暗号化、復号化、プロキシ、コンテンツ変換、プロトコル変換等のネットワーク接続装置２０上で行わないサービス処理を行うようにしてもよい。

【００９９】

以上のように本実施例においては、ネットワーク接続装置２０にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置２０が果たすようにする。これにより、第１の実施例と同様、サーバのＣＰＵの使用率を下げることができる。また、第１の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。さらに、処理振分部２６にパケットをサーバへ転送する機能を設けるとともに、サーバ１１に外部サービス処理部１５を設け、サービス処理を、ネットワーク接続装置２０とサーバ１１の両方で実行できるようにしたので、ネットワーク接続装置２０上で実現するのは困難なサービス処理をサーバ１１で行うことができ、ネットワークサービスが複雑な処理を必要とする場合でも対応することができる。

【０１００】

次に、第５実施例について説明する。図２０は本発明の第５の実施例のパケット中継処理装置の構成を示す図である。図２１に示すように、本実施例に係わるパケット中継処理装置は、第３実施例に係わるパケット中継処理装置を構成するサーバ１１にパケット詳細解析部１６を更に備える。このように構成することにより、ネットワーク接続装置２０の処理振分部２６が、与えられた条件によってパケットをサーバ１１に転送し、サーバ１１内のパケット詳細解析部１６がパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接続装置２０に設定する。そして、設定以後同じセッションに対して、ネットワーク接

続装置２０は、上記決定されたサービス内容に基づき中継処理を行うようにしたものである。

【０１０１】

図２０において、１１はサーバであり、サーバ１１は前記第３、第４の実施例と同様、サービス制御部１４を備えており、サービス制御部１４は、前記したように制御情報通信部３１を通して、ネットワーク接続装置２０のポリシーテーブル２５にポリシーを書き込む。更に、サービス制御部１４は、サーバ１１が備える詳細解析用ポリシーテーブル（図２０では不図示）にもポリシーを書き込む。

【０１０２】

また、サーバ１１はパケット詳細解析部１６を備えており、パケット詳細解析部１６は、不図示のパケット詳細解析用のセッションテーブル及びポリシーテーブルに基づいて、パケットを解析してそのパケットを含むセッションに対するサービスを決定し、決定したサービス内容をネットワーク接続装置２０のセッションテーブル２２ａ’のセッションデータを設定しなおす。再設定後、ネットワーク接続装置２０は上記サービス内容に基づき中継処理を行う。詳細解析用のセッションテーブル及びポリシーテーブルのデータ構成については後述する。

【０１０３】

第３及び第４実施例のサービス処理部２７や外部サービス処理部１５と同様に、パケット詳細解析部１６も、適用サービスタイプに応じてサーバ１１に複数備えられる。従って、新たなサービスタイプが必要になった場合、新たなサービスタイプに対応する新たなパケット詳細解析部１６をサーバ１１に追加することにより、容易に対応することが可能である。

【０１０４】

２０はネットワーク接続装置であり、本実施例のネットワーク接続装置２０は、第３の実施例と同様、パケット処理部２１、セッション管理部２２、セッションテーブル２２ａ’、ポリシーテーブル２５、処理振分部２６、サービス処理部２７を備えており、さらに処理振分部２６はパケットをサーバへ転送する機能を備えている。

【０１０５】

上記パケット処理部２１、セッション管理部２２、処理振分部２６、サービス処理部２７の動作は前記第３の実施例と同様である。本実施例に係わるポリシーテーブル２５のデータ構成は第３実施例と同様であるため、説明は省略する。本実施例にかかわるセッションテーブル２２ａ’のデータ構成については、後述する。

【０１０６】

また、本実施例においては、予めサーバ１１によりポリシーテーブル２５の適用サービスの欄に、上記パケット詳細解析部１６に転送するパケットと適用サービスの適用範囲（例えばｈｔｔｐはＵＲＬフィルタリング適用対象のパケットである等）を設定する。処理振分部２６は、前記第４の実施例で説明したのと同様に、ポリシーテーブル２５を参照してサーバ１１に転送するパケットを判断し、該当パケットのヘッダに適用サービスタイプの種類を付した後、そのパケットをパケット通信路３３を介してサーバ１１のパケット詳細解析部１６に転送する。

【０１０７】

以下、図２１から図２６を用いて、本実施例にかかわる各テーブルのデータ構成について説明する。まず、図２１から図２４を用いて本実施例にかかわるセッションテーブル２２ａ’について説明する。図２１から図２４に示すように、セッションテーブル２２ａ’に格納されるセッションデータに含まれる項目は、図１３に示すセッションテーブル２２ａ’と同様である。しかし、本実施例によれば、セッションデータがセッションテーブル２２ａ’に登録された後、パケット詳細解析部１６が、パケットを解析し、解析結果に基づいてセッションテーブル２２ａ’のセッションデータを再設定する。

【０１０８】

図２１及び図２２に、セッション管理部２２が、ポリシーテーブル２５に基づいてセッションデータを登録した際のセッションテーブル２２ａ’の一例を示す。図２１から図２２に示すように、まだパケット詳細解析部１６による解析が行われていないため、各セッションデータの適用サービスタイプの欄において、「サーバ転送：ＯＮ」となっている。従って、セッションデータに対応するセッションのパケットは、サーバ１１に転送される。

【０１０９】

図２３及び図２４に、パケット詳細解析部１６が、パケットの解析結果に基づいてセッションデータを再設定した後のセッションテーブル２２ａ’の一例を示す。図２３及び図２４に示すように、パケット詳細解析部１６による解析が行われたため、各セッションデータの適用サービスタイプの欄において、「サーバ転送：ＯＦＦ」となっている。従って、以後、各セッションデータに対応するセッションのパケットは、サーバ１１に転送されない事となる。

【０１１０】

また、パケット詳細解析部１６によってセッションデータが再設定された結果、図２１及び図２２に示すセッションテーブル２２ａ’と、図２３及び図２４に示すセッションテーブル２２ａ’とは、さらに、以下の点が異なる。

【０１１１】

・図２１に示すようにセッションＩＤ＝０及び１であるセッションデータの適用サービスタイプの欄に「ＵＲＬフィルタリング」が格納されている。一方、パケット詳細解析部１６によるパケット解析の結果、パケットを通過させることが決定されたため、図２３に示す同じセッションＩＤのセッションデータの同欄には、「フィルタリング通過」が格納されている。

【０１１２】

・図２１に示すように、セッションＩＤ＝２から５であるセッションデータの適用サービスタイプの欄に「ＵＲＬ負荷分散」が格納されているが、固有情報の欄に振分先サーバに関する情報は格納されていない。一方、パケット詳細解析部１６によるパケット解析の結果、振分先サーバが決定されたため、図２３に示すように、セッションＩＤ＝３及び４であるセッションデータは削除され、セッションＩＤ＝２及び５であるセッションデータの適用サービスタイプの欄に「ヘッダ書換」が格納され、固有情報の欄に振分先サーバに関する情報が格納されている。

【０１１３】

・図２２に示すように、セッションＩＤ＝６及び７であるセッションデータの適用サービスタイプの欄に「ＦＴＰ（File Transfer Protocol）フィルタリング

」が格納されている。その後パケット詳細解析部１６によるパケット解析の結果、そのセッションのパケットを通過させると決定されたため、図２４に示すように、セッションＩＤ＝６及び７である制御コネクションのためのセッションデータに加えて、新たにセッションＩＤ＝８及び９であるデータコネクションのためのセッションデータが登録され、そのセッションデータの適用サービスタイプの欄に「フィルタリング通過」が格納されている。

【０１１４】

次に、図２５及び図２６を用いて、パケット詳細解析部１６が備えるテーブルについて説明する。パケット詳細解析部１６は、パケットを解析するために、詳細解析用セッションテーブル及び詳細解析用ポリシーテーブルを備える。

【０１１５】

図２５に、詳細解析用セッションテーブルの構成例を示す。図２５に示す詳細解析用セッションテーブルは、図２１及び図２２に示すセッションテーブル２２ａ’に対応する。図２５に示すように、詳細解析用セッションテーブルに格納されるセッションデータは、セッションＩＤ、セッション検索キー、セッション状態、関連セッション及び適用サービスタイプを項目として含む。関連セッション以外の項目は、セッションテーブル２２ａ’に格納されるセッションデータと同様である。関連セッションは、パケット詳細解析部１６がパケットを解析した結果、関連すると判定されたセッションのセッションＩＤである。詳細解析用セッションテーブル内のセッションデータは、セッションテーブル２２ａ’に格納されるセッションデータに基づいて、詳細解析を行う際にパケット詳細解析部１６によって登録され、詳細解析が終了するとパケット詳細解析部１６によって削除される。

【０１１６】

図２６に、詳細解析用ポリシーテーブルの構成例を示す。図２６に示す詳細解析用ポリシーテーブルは、図１４に示すポリシーテーブル２５よりも詳しいポリシーを格納する。例えば、ＵＲＬフィルタリングについては、ＵＲＬ毎にパケットを廃棄するか否かを示すＵＲＬフィルタリング用ＵＲＬテーブルが詳細解析用ポリシーテーブルに備えられる。また、例えばＦＴＰフィルタリングについては

、ＩＰアドレス及びポート番号ごとに、パケットを通過させるべきか廃棄させるべきかを示すＦＴＰフィルタリング用テーブルが備えられる。更にまた、例えば、ＵＲＬ負荷分散については、ＵＲＬ毎に振分先サーバの候補のＩＰアドレス及び振分方法を示すＵＲＬ負荷分散用テーブル等が備えられる。なお、図２５に示す詳細解析用セッションテーブルは、図２１から図２４に示すセッションテーブル２２ａ’に対応している。

【０１１７】

以下、図２７を用いて第５実施例に係わるパケット中継処理装置の動作概念について説明する。図２７において、実線の矢印は、パケットの進む方向を示し、破線の矢印は、テーブル内のデータの読み込み及びテーブルへのデータ書き込みを示す。

【０１１８】

まず、サーバ１１内のサービス制御部１４は、制御情報通信部３１を介して、ネットワーク接続装置２０のポリシーテーブル２５及びパケット詳細解析部１６内の詳細解析用ポリシーテーブルにポリシーを書き込む（矢印Ａ１１）。

【０１１９】

続いて、ネットワーク接続装置２０にパケットが入力されると、セッション管理部２２は、パケットのヘッダに格納された情報を用いてポリシーテーブル２５を参照し、ヘッダ内の情報とポリシー検索キーがマッチするポリシーを取得し、そのポリシーに基づいてセッションデータを作成し、セッションテーブル２２ａ’に格納する（矢印Ａ１２）。

【０１２０】

そのセッションデータの適用サービスタイプの欄に「サーバ転送：ＯＮ」が格納されている場合、処理振分部２６は、パケット通信部３３を介してそのパケットをパケット詳細解析部１６に転送する。パケット詳細解析１６は、詳細解析用ポリシーテーブル及び詳細解析用セッションテーブルを用いてそのパケットを解析する（矢印Ａ１３）。パケット詳細解析部１６は、パケットの解析結果に基づいて、ネットワーク接続装置２０内のセッションテーブル２２ａ’に格納されたセッションデータを再設定する（矢印Ａ１４）。パケットの解析後は、ネットワ

ーク接続装置２０に入力したパケットは、パケット詳細解析部１６によって解析されることなく、サービス処理部２７によって処理され、ネットワーク接続装置２０から出力される（矢印Ａ１５）。

【０１２１】

以下、第５実施例に係わるパケット中継処理装置の動作について説明する。パケット処理部２１及びセッション管理部２２による処理の手順は、第１から第４実施例と同様であるため、説明を省略する。以下、処理振分部２６、サービス処理部２７及びパケット詳細解析部１６による処理の手順に重点をおいて説明する。

【０１２２】

図２８は処理振分部２６及びサービス処理部２７の処理フローを示す図である。図２８に示す処理のうち、ヘッダ書換処理（ステップＳ６４）までの処理は図１９と同じである。さらに、第５実施例によれば、処理振分部２６は、セッションデータに含まれる適用サービスタイプに基づいて、入力パケットがサーバ１１に転送するべき該当パケットであるか否かを判断する（ステップＳ８１）。適用サービスタイプに「サーバ転送：ＯＮ」及び適用サービスタイプが設定されている場合には、振分処理部２６は、そのパケットをサーバ１１に転送するべきパケットであると判断し（ステップＳ８１：Ｙｅｓ）、パケットに転送用ヘッダを付す処理を行うサービス処理部２７に、処理を振り分ける。処理を振り分けられたサービス処理部２７は、そのパケットに転送用ヘッダを付す。転送用ヘッダの内容は第４実施例と同様である。転送用ヘッダを付されたパケットは、パケット通信部３３を介して、サーバ１１のパケット詳細解析部１６に転送される（ステップＳ８２）。パケット詳細解析部１６は、受信したパケットを解析し、解析結果に基づいて、制御情報通信部３１を介して、セッションテーブル２２ａ’に格納されたセッションデータを再設定する（ステップＳ８３）。

【０１２３】

図２９は、パケット詳細解析部１６の処理の手順を示すフローチャートである。図２９に示す処理は、図２８のステップＳ８３に相当する。本実施例においては、例として、ＵＲＬフィルタリング、ＵＲＬ負荷分散、及びＦＴＰフィルタリ

ングサービスをパケット詳細解析部１６を用いて提供する場合について説明する。

【０１２４】

まず、ＵＲＬフィルタリングサービスについて説明する。

予めサーバ１１のサービス制御部１４が、「パケット詳細解析部１６へパケットを転送しＵＲＬフィルタリングを行う」というポリシーを、制御通信情報部３１を介してポリシーテーブル２５に設定する。

【０１２５】

設定された条件から、ネットワーク接続装置２０の処理振分部２６が、該当パケットをパケット詳細解析部１６に転送する。

パケット詳細解析部１６では、受信したパケットの転送用ヘッダ内に含まれる適用サービスタイプ「ＵＲＬフィルタリング」に基づいて、そのパケットがＵＲＬフィルタリングサービスを受けるべきパケットであることを判定する。パケット詳細解析部１６は、受信したパケットに含まれる情報に基づいてセッションデータを作成し、詳細解析用セッションテーブルに格納する（ステップＳ９１：Ｙｅｓ）。以後、パケット詳細解析部１６は、そのセッションの状態を管理し、ＨＴＴＰのＧＥＴリクエストを受信するまで、受信したパケットをそのままネットワークへ出力させる。

【０１２６】

セッション状態がＥＳＴＡＢとなった後、ＨＴＴＰのＧＥＴリクエストを受信した場合（ステップＳ９２：Ｙｅｓ）、パケット詳細解析部１６は、ＵＲＬを判定し、パケットの通過／廃棄を決定する。すなわち、パケット詳細解析部１６は、そのパケットに含まれるＵＲＬを用いて、予め設定された詳細解析用ポリシーテーブルに含まれるＵＲＬフィルタリング用ＵＲＬテーブルを参照することにより、そのパケットの通過／廃棄を判定する（ステップＳ９３）。

【０１２７】

パケットを廃棄すると判定した場合には（ステップＳ９３：Ｙｅｓ）、パケット詳細解析部１６は、そのセッションのパケットを廃棄する（ステップＳ１０３）。更に、パケット詳細解析部１６は、パケットに含まれるセッションＩＤを用

いてセッションテーブル２２ａ’を参照し、セッションＩＤに対応するセッションデータの適用サービスタイプの欄を、「サーバ転送：ＯＮ・ＵＲＬフィルタリング」から「廃棄」に書き換える（不図示）。

【０１２８】

また、パケットを通過させると判定したの場合には（ステップＳ９３：Ｎｏ）、パケット詳細解析部１６は、セッションテーブル２２ａ’を参照し、パケットに含まれるセッションＩＤに対応するセッションデータの適用サービスタイプの欄を「サーバ転送：ＯＮ・ＵＲＬフィルタリング」から「フィルタリング通過」に書き換える（ステップＳ９４）。図２１及び図２３に示すセッションテーブル２２ａ’においてセッションＩＤ＝０及び１であるセッションデータは、それぞれ、ＵＲＬフィルタリングの場合の、パケット解析前後のセッションデータの一例である。

【０１２９】

セッションテーブル２２ａ’内のセッションデータを再設定した後、パケット詳細解析部１６は、詳細解析用セッションテーブルから、そのセッションＩＤに対応するセッションデータを削除する（不図示）。

【０１３０】

上記のように、パケット詳細解析部１６が、ネットワーク接続装置２０のセッションテーブル２２ａ’内のセッションデータの適用サービスタイプを、「サーバ転送：ＯＮ」から「フィルタリング通過」または「廃棄」に設定し直すと、ネットワーク接続装置２０は上記通過条件に従い、以後のパケットを処理する。すなわち、ネットワーク接続装置２０は、サーバ１１のパケット詳細解析部１６にパケットを転送することなく、パケットを通過させたり、廃棄する。

【０１３１】

図３０は、上記ＵＲＬフィルタリングの動作を説明する図である。

クライアント、サーバ間で、ＳＹＮ、ＳＹＮ＿ＡＣＫ、ＡＣＫパケットを交換する。そのセッションがＥＳＴＡＢの状態に遷移するまでは、ネットワーク接続装置２０から上記パケット詳細解析部１６にそれらパケットが転送され、パケット詳細解析部１６は、そのセッションの状態を管理する。つまり、「ネットワー

ク接続装置２０」及び「サーバ１１」で処理が行われる。

【０１３２】

セッションがＥＳＴＡＢ状態に遷移し、ＨＴＴＰのＧＥＴリクエスト（ＧＥＴ”ｈｔｔｐ：／／ｗｗｗ．ｘｘｘ．ｃｏ．ｊｐ”のようにＵＲＬが付されている）を受信すると、サーバ１１のパケット詳細解析部１６は、詳細解析用ポリシーに含まれるＵＲＬフィルタリング用ＵＲＬテーブルを参照して上記ＵＲＬのパケットが廃棄するべきパケットであるか通過させるべきパケットであるかを判定し、判定結果に基づいてセッションテーブル２２ａ’の適用サービスタイプの欄のエントリを「廃棄」または「通過」に書き換える。

【０１３３】

以後、ネットワーク接続装置２０は、セッションテーブル２２ａ’に設定された適用サービスタイプに応じて、そのセッションが終了するまで、パケットを廃棄または通過させる。つまり、「ネットワーク接続装置２０」で処理が行われる。

【０１３４】

次に、図２９に戻って、ＵＲＬ負荷分散サービスについて説明する。

ＵＲＬ負荷分散において、例えば、クライアントがある代表サーバにアクセスした後に、ＵＲＬに基づいて代表サーバに接続された他のサーバを振分先サーバとして決定し、その振分先サーバにセッションを振り分けることにより、負荷を複数の振分先サーバに分散させることができる。

【０１３５】

ＵＲＬ負荷分散を行う際、まずサーバ１１のサービス制御部１４が、「パケット詳細解析部１６へパケットを転送しＵＲＬ負荷分散を行う」というポリシーを、制御通信情報部３１を介してポリシーテーブル２５の適用サービスタイプ欄に設定する。

【０１３６】

設定された条件から、ネットワーク接続装置２０の処理振分部２６が該当パケットをサーバ１１のパケット詳細解析部１６に転送する。

パケット詳細解析部１６では、受信したパケットに含まれる適用サービスタイ

プ「ＵＲＬ負荷分散」に基づいて、そのパケットがＵＲＬ負荷分散サービスを受けるべきパケットであることを判定する。パケット詳細解析部１６は、ＵＲＬフィルタリングの場合と同様にして、受信したパケットに含まれる情報に基づいてセッションデータを作成し、詳細解析用セッションテーブルに格納する。さらに、パケット詳細解析部１６は、パケットのヘッダに含まれる送信元アドレス、宛先アドレス及びポート番号等に基づいて代理応答を行い、相互に関連するセッションデータを登録し、セッションデータの関連セッションの欄に、関連するセッションデータのセッションＩＤを格納する（ステップＳ９５：Ｙｅｓ）。

【０１３７】

図２５に示す詳細解析用セッションテーブルにおいて、セッションＩＤ＝２から５であるセッションデータは、ＵＲＬ負荷分散の場合のセッションデータの一例である。図２５において、セッションＩＤ＝２であるセッションデータは、セッションＩＤ＝４であるセッションデータと相互に関連し、セッションＩＤ＝３であるセッションデータは、セッションＩＤ＝５であるセッションデータと相互に関連している事がわかる。

【０１３８】

パケット詳細解析部１６では、クライアントとサーバ１１の間にコネクションを確立し、以後、セッションの状態を管理する。また、パケット詳細解析部１６は、ＴＣＰ（Transmission Control Protocol ）を終端する機能を有し、振分先サーバが決定するまで、パケット詳細解析部１６は、振分先サーバの変わりにクライアントに対する応答を行う。パケット詳細解析部１６は、セッションの状態がＥＳＴＡＢとなった後、ＨＴＴＰのＧＥＴリクエストを受信した場合（ステップＳ９６：Ｙｅｓ）、パケット詳細解析部１６は、パケットに含まれるＵＲＬを用いて、予め設定された詳細解析用ポリシーテーブルに含まれるＵＲＬ負荷分散用テーブルを参照して、振分先サーバを決定する（ステップＳ９７）。その後、サーバ１１は、ＳＹＮ、ＳＹＮ＿ＡＣＫ、ＡＣＫパケットを交換することにより、振分先サーバとコネクションを確立する。

【０１３９】

さらに、パケット詳細解析部１６は、ネットワーク接続装置２０のセッション

データ２２ａ’を参照し、パケットに含まれるセッションＩＤに対応するセッションデータを取得する。そして、パケット詳細解析部１６は、取得したセッションデータに含まれる適用サービスタイプを「サーバ転送：ＯＮ・ＵＲＬ負荷分散」から「サーバ転送：ＯＦＦ・ヘッダ書換」に書き換える。さらに、パケット詳細解析部１６は、セッションデータの固有情報の欄に、決定された振分先サーバのＩＰアドレス等に従って、ＩＰアドレス：ポート番号、およびシーケンス番号／ＡＣＫ番号差分を設定する（ステップＳ９８）。これにより、相互に関連していると判定された２つのセッションデータを１つのセッションデータにまとめることになるため、２つのコネクションを１つのコネクションとして扱うことが可能となる。さらに、パケット詳細解析部１６は、４つのセッションデータのうち、不要になった残りの２つのデータを、セッションテーブル２２ａ’から削除する。

【０１４０】

セッションテーブル２２ａ’内のセッションデータを再設定した後、パケット詳細解析部１６は、詳細解析用セッションテーブルから、そのセッションＩＤに対応するセッションデータを削除する（不図示）。そして、サーバ１１は、振分先サーバにＨＴＴＰのＧＥＴリクエストを送出する。

【０１４１】

図２１及び図２３に示すセッションテーブル２２ａ’内のセッションＩＤ＝２から５であるセッションデータは、それぞれ、ＵＲＬ負荷分散の場合のパケット解析前後のセッションデータの一例である。図２１におけるセッションＩＤ＝２及び４である２つのセッションデータによって示される２つのコネクションは、図２３において、セッションＩＤ＝２であるセッションデータで示される１つのコネクションにまとめられている。同様に、図２１におけるセッションＩＤ＝３及び５である２つのセッションデータによって示される２つのコネクションは、図２３において、セッションＩＤ＝５であるセッションデータで示される１つのコネクションにまとめられている。

【０１４２】

パケットの解析後、パケットは、パケット詳細解析部１６に送られない。ネッ

トワーク接続装置２０のヘッダ書換処理を行うサービス処理部２７は、セッションテーブル２２ａ’に格納されたセッションデータ内の固有情報に基づいて、パケット内のＩＰアドレス：ポート番号、シーケンス番号、ＡＣＫ番号を書き換えた後、そのパケットをネットワークに出力させる。

【０１４３】

図３１は、上記ＵＲＬ負荷分散サービスの動作を説明する図である。

図３１に示すように、クライアントとパケット中継処理装置の間でＳＹＮ、ＳＹＮ＿ＡＣＫ、ＡＣＫパケットを交換する。セッションがＥＳＴＡＢ状態に遷移し、ＨＴＴＰのＧＥＴリクエストを受信すると、パケット詳細解析部１６は、ＧＥＴリクエストのＵＲＬを判定し、振分先サーバを決定する。

【０１４４】

ついで、上記と同様に、パケット中継処理装置と振分先サーバの間でＳＹＮ、ＳＹＮ＿ＡＣＫ、ＡＣＫパケットを交換し、振分先サーバにＨＴＴＰのＧＥＴリクエストを送出する。ここまでは、「ネットワーク接続装置２０」＋「サーバ１１」で処理が行われる。

【０１４５】

パケット中継処理装置から振分先サーバにＨＴＴＰのＧＥＴリクエストを送出した後、セッションが終了するまで、ネットワーク接続装置２０が、セッションテーブル２２ａ’に格納されたセッションデータに基づいて、クライアントと振分先サーバとの間の中継処理を行う。

【０１４６】

次に、図２９に戻って、ＦＴＰフィルタリングサービスについて説明する。ＦＴＰは、制御用の制御コネクションと、１以上のデータ転送用のデータコネクションとの複数のＴＣＰコネクションからなる。

【０１４７】

予めサーバ１１のサービス制御部１４が、「パケット詳細解析部１６へパケットを転送しＦＴＰフィルタリングを行う」というポリシーを、制御通信情報部を介してポリシーテーブル２５に設定する。

【０１４８】

設定された条件から、ネットワーク接続装置２０の処理振分部２６が該当パケットを詳細解析部１６に転送する。ＵＲＬフィルタリングの場合と同様に、パケット詳細解析部１６は、受信したパケットに含まれる適用サービスタイプに基づいて、そのパケットがＦＴＰフィルタリングサービスを受けるべきパケットであることを判定し、パケット詳細解析部１６は、詳細解析用セッションテーブルにセッションデータを格納する（ステップＳ９９：Ｙｅｓ）。続いて、パケット詳細解析部１６は、セッション状態を管理し、受信パケットをそのままネットワークへ出力させる。

【０１４９】

セッション状態がＥＳＴＡＢとなった後、図３２に示すように、ＦＴＰのＰＯＲＴ命令もしくは、ＰＡＳＶ命令のＡＣＫパケットを受信すると（ステップＳ１００：Ｙｅｓ）、パケット詳細解析部１６は、そのパケットに含まれるＩＰアドレスとポート番号を判定し、判定結果に基づいて、そのセッションのパケットを通過するか廃棄するかを決定する（ステップＳ１０１）。

【０１５０】

すなわち、パケット詳細解析部１６は、ＩＰアドレスとポート番号を用いて予め設定された詳細解析用ポリシーテーブル内のＦＴＰフィルタリング用テーブルを参照して、そのセッションのパケットを通過させるか廃棄するかを決定する。パケットを廃棄すると決定した場合には（ステップＳ１０１：Ｙｅｓ）、パケット詳細解析部１６は、セッションテーブル２２ａ’からパケットの転送用ヘッダに含まれるセッションＩＤに対応するセッションデータを取得し、そのセッションデータの適用サービスタイプの欄に「廃棄」を設定し、そのパケットを廃棄する（ステップＳ１０３）。

【０１５１】

また、そのパケットを通過させると決定した場合には（ステップＳ１０１：Ｎｏ）、パケット詳細解析部１６は、先のＰＯＲＴ命令もしくはＰＡＳＶ命令のＡＣＫパケットのデータ部分に記述されているＩＰアドレスとポート番号に基づいて、データコネクションについてのセッションデータをセッションテーブル２２ａ’に登録し、そのセッションデータの適用サービスタイプの欄に「フィルタリ

ング通過」を設定する（ステップＳ１０２）。

【０１５２】

上記のようにパケット詳細解析部１６が、セッションテーブル２２ａ’内のセッションデータを再設定すると、ネットワーク接続装置２０は上記通過条件に従い、以後のデータコネクションに関するパケットを処理する。すなわち、サーバ１１のパケット詳細解析部１６にパケットを転送することなく、パケットを通過させたり、廃棄させたりする。

【０１５３】

図３２は、上記ＦＴＰフィルタリングの動作を説明する図である。クライアント、サーバ１１間で、ＳＹＮ、ＳＹＮ＿ＡＣＫ、ＡＣＫパケットを交換し、ＥＳＴＡＢの状態に遷移するまでは、上記パケット詳細解析部１６にパケットが転送され、「ネットワーク接続装置２０」＋「サーバ１１」で処理が行われる。

【０１５４】

セッションの状態がＥＳＴＡＢ状態に遷移し、ＦＴＰのＰＯＲＴ命令またはＰＡＳＶ命令のＡＣＫ（ＩＰアドレスとポート番号が付されている）を受信すると、パケット詳細解析部１６は、パケットに含まれるＩＰアドレスとポート番号を用いて詳細解析用ポリシーテーブルを参照し、そのパケットを廃棄すべきか、通過させるべきかを決定する。そのパケットを廃棄すると決定する場合には、パケット詳細解析部１６は、セッションテーブル２２ａ’のセッションデータにパケットを廃棄する旨を設定する。そのパケットを通過させると決定する場合には、パケット詳細解析部１６は、セッションテーブル２２ａ’にデータコネクションについてのセッションデータを登録し、適用サービスタイプ欄に「通過」を設定し直す。以後、ネットワーク接続装置２０は、パケットの廃棄処理又はデータコネクションのパケットの通過処理を行う。

【０１５５】

最後に、パケット中継処理装置がクライアントから制御コネクションのＦＩＮパケットを受信すると、ネットワーク接続装置２０からパケット通信部３３を介して、サーバ１１のセッション詳細解析部１６にそのパケットが転送される。サーバ１１は、セッション詳細解析部１６を介してそのセッションのクローズ処理

を行う。さらに、セッション詳細解析部１６は、パケットの転送用ヘッダに含まれるセッションＩＤに基づいて、クローズされるセッションに関するセッションデータを削除する。

【０１５６】

以下、図３３及び図３４を用いて、第５実施例におけるパケットのフローについて、ＵＲＬ負荷分散サービスの場合を例にとって説明する。なお、各図は、図２１、図２３、図２５に示すセッションテーブルに格納されたセッションＩＤ＝２から５のセッションデータに対応する。図３３に、パケット詳細解析部１６によってセッションデータが再設定される前のパケットフローを示す。

【０１５７】

セッションデータが再設定される前において、矢印Ａ２１に示すように、アドレス：ポート番号が192.168.30.30:11950 であるクライアントからネットワーク接続装置２０へ「宛先アドレス：ポート番号＝192.168.200.1:http、送信元アドレス：ポート番号＝192.168.30.30:11950」をヘッダに格納したパケットＰ１１が送信される。ネットワーク接続装置２０のセッション管理部２２は、ポリシーテーブル２５を参照し、ヘッダ内の情報とポリシー検索キーがマッチするポリシーを取得し、そのポリシーに基づいてセッションＩＤ＝２であるセッションデータを作成し、セッションテーブル２２ａ’に格納する。

【０１５８】

セッションデータ内の適用サービスタイプは「サーバ転送：ＯＮ・ＵＲＬ負荷分散」であるため、ネットワーク接続装置２０内の処理振分部２６は、サーバ転送処理を行うサービス処理部２７に処理を振り分ける。処理を振り分けられたサービス処理部２７がそのパケットに転送用ヘッダを付したのち、矢印Ａ２２に示すようにパケットはサーバ１１に転送される。サーバ１１のパケット詳細解析部１６は、転送されたパケットに含まれる情報に基づいて、詳細解析用セッションテーブルにセッションデータを登録する。

【０１５９】

同様にして、サーバ１１からクライアントへ矢印Ａ２３からＡ２８に示すような経路を経てパケットＰ１２、Ｐ１３及びＰ１４が出力される際に、それぞれ、

セッションＩＤ＝３、４及び５であるセッションデータが、セッションテーブル２２ａ’にセッション管理部２２によって格納され、対応するセッションデータが、詳細解析用セッションテーブルにパケット詳細解析部１６によって格納される。

【０１６０】

セッションデータを各セッションテーブルに登録した後、ＨＴＴＰのＧＥＴリクエストを受信するまで、パケット詳細解析部１６は、各セッションの状態を管理し、図３３に示すパケットフローに基づいて、受信したパケットをネットワークへ出力する。

【０１６１】

その後、セッション状態がＥＳＴＡＢとなった後、ＨＴＴＰのＧＥＴリクエストを受信すると、パケット詳細解析部１６は、パケットを解析し、解析結果に基づいて、セッションテーブル２２ａ’に格納されたセッションデータを設定しなおす。再設定後のセッションデータは、図２３に示す通りである。

【０１６２】

図３４に、パケット詳細解析部１６によってセッションデータが再設定された後のパケットフローを示す。セッションデータが再設定された後において、矢印Ａ３１に示すように、振分先サーバからネットワーク接続装置２０へ「宛先アドレス：ポート番号として192.168.200.1:3333、送信元アドレス：ポート番号として192.168.200.10:8080」をヘッダに格納したパケットＰ１４が送信されると、ネットワーク接続装置２０の処理振分部２６は、パケットのヘッダに含まれる情報を用いて、セッションテーブル２２ａ’を参照し、セッションＩＤ＝５であるセッションデータを取得し、セッションデータに基づいて、ヘッダ書換処理を行うサービス処理部２７に処理を振り分ける。サービス処理部２７は、そのセッションデータに基づいて、そのパケットのヘッダ内の宛先アドレス及びポート番号を「192.168.30.30:11950」に、クライアントのアドレス及びポート番号を「192.168.200.1:http 」に書き換えることにより、パケットＰ１２を作成する。その後、矢印Ａ３２に示すように、ネットワーク接続装置２０は、パケットＰ１２を振分先サーバへそのパケットを出力する。

【０１６３】

同様に、矢印Ａ３３に示すように、アドレス：ポート番号が192.168.30.30:11950 であるクライアントからネットワーク接続装置２０へ「宛先アドレス：ポート番号＝192.168.200.1:http、送信元アドレス：ポート番号＝192.168.30.30:11950」をヘッダに格納したパケットＰ１１が送信される。ネットワーク接続装置２０の処理振分部２６は、パケットのヘッダに含まれる情報を用いて、セッションテーブル２２ａ’を参照し、セッションＩＤ＝２であるセッションデータを取得する。この例の場合、取得したセッションデータの適用サービスタイプの欄に「サーバ転送：ＯＦＦ／ヘッダ書換」が格納されているため、処理振分部２６は、ヘッダ書換処理を行うサービス処理部２７に処理を振り分ける。サービス処理部２７は、そのセッションデータに基づいて、そのパケットのヘッダ内の宛先アドレス及びポート番号を振分先サーバのアドレス及びポート番号を「192.168.200.10：8080」に書き換えることにより、パケットＰ１３を作成する。その後、ネットワーク接続装置２０は、矢印Ａ３４に示すように、パケットＰ１３を振分先サーバへそのパケットを出力する。

【０１６４】

このように、セッション詳細解析部１６がパケットの解析結果に基づいてセッションデータを書き換えた後は、サーバ１１を介さずに、ネットワーク接続装置２０によってパケットの中継処理が行われる。

【０１６５】

以上のように、本実施例においては、ネットワーク接続装置２０にセッション管理に基づくパケット中継処理機能を設け、従来サーバ上に配置していた機能をネットワーク接続装置２０が果たすようにしたので、第１の実施例と同様、サーバ１１のＣＰＵの使用率を下げることができる。また、第１の実施例と同様、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

【０１６６】

さらに、第５実施例によれば、サーバ１１のパケット詳細解析部１６においてパケットを解析してサービスを決定し、決定したサービス内容をネットワーク接

続装置２０に設定し、以後同じセッションに対してネットワーク接続装置２０が上記決定されたサービス内容に基づき中継処理を行うようにする。従って、サーバ１１で全ての処理を行う場合に比べ、サービス処理を高速に実現することができる。

【０１６７】

以下、各実施例の変形例について説明する。まず、第１の変形例について説明する。第１実施例から第５実施例において、第１の変形例を適用することにより、セッションが終了した後すぐにセッションデータを削除するのではなく、一定時間経過した後にセッションデータをセッションテーブル２２ａ’することとしてもよい。

【０１６８】

そのために、第１の変形例によれば、図１３及び図１４、図２１から図２４に示すように、ポリシーテーブル２５及びセッションテーブル２２ａ’のエントリに、さらに一貫性保持時間を含む。以下、第１の変形例に係わるパケット中継処理装置が行う処理について説明する。第１の変形例では、セッション管理部２２が行う処理の一部が第１から第５実施例と異なる。第１の変形例を適用した場合のセッション管理部２２が行う処理について、図５を用いて説明する。

【０１６９】

図５のステップＳ１７において、セッション管理部２２が、あるセッションがクローズしたと判定した場合（ステップＳ１７：Ｙｅｓ）、セッション管理部２２はタイマーを設定する。セッション管理部２２は、セッションデータに含まれる一貫性保持時間だけ待機した後に、図５のステップＳ１８に進み、そのセッションデータをセッションテーブル２２ａ’から削除する。

【０１７０】

これにより、セッションが終了した後で、一貫性保持時間が経過するまでの間に、そのセッションが再度確立された場合、セッション検索キーに変更がなければ、セッション管理部２２は、そのセッションを先に終了したセッションと同じセッションとして扱う事ができるようになる。例えば、負荷分散サービスにおいて、一度終了したセッションと再度確立されたセッションとで同じ振分先サーバ

にパケットを振り分けることが可能となる。延いては、セッション管理部２２によるポリシーテーブル２５の検索や処理振分部２６によるパケットのサーバ１１への転送を省略する事ができるため、高速にパケットを処理することが可能となる。

【０１７１】

次に、第２の変形例について説明する。第３実施例から第５実施例において、第２の変形例を適用することにより、セッションに適用するポリシーの切り換えが容易にできるようにすることとしてもよい。そのために、第２の変形例によれば、複数のポリシーをいくつかのグループに分ける。さらに、図１４に示すように、ポリシーテーブル２５に格納されるポリシーは更に項目として、そのポリシーが属するグループを識別するグループＩＤを含み、ネットワーク接続装置２０は、更に図３５に示すフラグテーブルを備える。

【０１７２】

以下、図３５を用いて、フラグテーブルのデータ構造について説明する。図３５に示すように、フラグテーブルは、グループＩＤに対応して、ポリシーの有効・無効を示すフラグを格納する。図３５において、例として、フラグが「オフ（０）」である場合にポリシーは無効であり、フラグが「オン（１）」である場合にポリシーは有効である。

【０１７３】

以下、第２の変形例に係わるパケット中継処理装置が行う処理について説明する。第２の変形例では、セッション管理部２２が行う処理の一部が第３から第５実施例と異なる。例として、第３実施例に係わるセッション管理部２２が行う処理を示す図１５を参照しながら、第２の変形例を各実施例に適用することにより、セッション管理部２２が行う処理が変化する点について詳しく説明する。

【０１７４】

第２の変形例において、セッション管理部２２は、図１５のステップＳ４３からステップＳ４４の間でさらに、以下の処理を行う。まず、ステップＳ４３で、セッション管理部２２は、ポリシーテーブル２５を検索し、パケットのヘッダに格納された情報と適合するポリシー検索キーを持つポリシーを取得する。セッシ

ョン管理部２２は、得られたポリシーに含まれるグループＩＤを用いてフラグテーブルを参照し、そのグループＩＤに対応するフラグがオンであるかオフであるか判定する。

【０１７５】

判定の結果、フラグがオフである場合、セッション管理部２２はそのポリシーを採用しない。一方、フラグがオンである場合、セッション管理部２２は、そのポリシーを採用する。セッション管理部２２は、ステップＳ４４で、そのポリシーに基づいてセッションデータを作成し、セッションテーブル２２ａ’に格納する。これにより、採用するべきポリシーをグループ毎に切り換えることができるようになる。

【０１７６】

例えば、複数の通常用のポリシーと複数の非常用のポリシーとを作成した場合、第２の変形例によれば、予め通常用のポリシーからなる通常用グループと、非常用のポリシーからなる非常用グループを定義し、ポリシーテーブル２５には、通常用のポリシーも非常用のポリシーも両方登録する。また、フラグテーブルにパケット中継処理装置のユーザが有効にしておきたいグループ、つまり、通常用と非常用いずれかのグループに対応するフラグをオンにする。これにより、通常用のポリシーと非常用のポリシーを、グループ毎に容易に切り換える事が可能となる。

【０１７７】

次に、第３の変形例について説明する。第３実施例から第５実施例において、第３の変形例を適用することにより、パケットのログを採取できるようにすることとしてもよい。そのために、第３の変形例によれば、図１３及び図１４並びに図２１から図２４に示すポリシーテーブル２５及びセッションテーブル２２ａ’に格納されるセッションデータ及びポリシーは、更に項目としてイベントフラグを含む。

【０１７８】

イベントフラグには、パケットに関するイベントフラグと、ヘッダに関するイベントフラグとがある。パケットに関するイベントフラグが「オン（１）」であ

る場合、ログ（履歴）を採取するために、そのパケットがサーバ１１に転送される。ヘッダに関するイベントフラグがオンである場合、ログを採取するために、そのパケットのヘッダがサーバ１１に転送される。サーバ１１は、転送されたパケット又はパケットのヘッダを解析し、ログを採取する。これにより、例えば、システムに障害が生じたときに、ネットワーク管理ソフトを用いて、採取したログを解析する事により、障害から復旧するために役に立つ情報を得ることが可能となる。

【０１７９】

次に、第４の変形例について説明する。第４の変形例によれば、第１実施例から第５実施例に係わるネットワーク接続装置２０は、パケットに関する統計情報を取得するために、更にカウンタ（不図示）を備える。上記サーバ１１のネットワーク制御部１２又はサービス制御部１４は、カウンタの値を参照する。統計情報として、例えば、インターフェースごとのパケット入力数と出力数が考えられる。この統計情報は、クライアント等に課金を行う際等において使用することができる。

【０１８０】

また、第３実施例から第５実施例に対しては、更に、統計情報として、ポリシーテーブル２５に格納されたポリシー毎に、そのポリシーが適用されたセッションの数、つまり、ポリシーがヒットした回数であるポリシーヒット数を得る事としても良い。

【０１８１】

そのために、第４の変形例によれば、図１４に示すように、ポリシーテーブル２５に格納されるポリシーは、更に項目としてポリシーヒット数を含む。そして、セッション管理部２２が、新たなセッションに関するセッションデータをセッションテーブル２２ａ’に登録するために、ポリシーテーブル２５を参照して適用するべきポリシーを取得すると、カウンタは、取得されたポリシーのポリシーヒット数をインクリメントする。これにより、ネットワーク管理者は、ポリシーが有効に利用されているか否かを判断するための情報を得る事が可能となる。

【０１８２】

また、第３実施例から第５実施例に対しては、更に、統計情報として、負荷分散サービスにおける振分先サーバ毎に、セッションが振り分けられた回数を示す振分先ヒット数を得る事としても良い。

【０１８３】

そのために、図１４に示すポリシーテーブル２５又は、図２６に示す詳細解析用ポリシーテーブルに格納された負荷分散サービスにかかわるポリシーは、更に項目として、振分先サーバアドレスごとの振分先ヒット数を含む。そして、サービス処理部２７又はパケット詳細解析部１６が、セッションの振分先サーバを決定する処理を行うごとに、カウンタは、振分先サーバとして決定されたサーバに対応する振分先ヒット数をインクリメントする。これにより、ネットワーク管理者は、負荷分散の振分方式が有効に動作しているか否かを判断するための情報を得ることが可能となる。

【０１８４】

本実施形態において説明したネットワーク接続装置２０を構成する各部及びサーバ１１を構成する各部が行う処理を示すプログラムは、それぞれＲＡＭ（Random Access Memory）やＲＯＭ（Read Only Memory）等のメモリに記録され、パケット中継処理装置にハードウェア或いはソフトウェアとして備えられても良い。以下、この場合について説明する。

【０１８５】

図３６にコンピュータ（情報処理装置）の構成を示す。図３６に示すように、コンピュータ４０は、少なくともＣＰＵ４１、メモリ４２を備える。さらに、コンピュータ４０は、入力装置４３、出力装置４４、外部記憶装置４５、媒体駆動装置４６、及びネットワークインターフェース４７を備えることとしても良い。各装置はバス４８により互いに接続されている。

【０１８６】

メモリ４２は、例えば、ＲＯＭ、ＲＡＭ等を含み、処理に用いられるプログラムとデータを格納する。ＣＰＵ４１は、メモリ４２を利用してプログラムを実行することにより、必要な処理を行う。

【０１８７】

２以上のコンピュータ４０に、パケット中継処理装置を構成するサーバ１１及びネットワーク接続装置２０に相当する機能を実現させる場合、まず、図２、１０、１２、１８、２０に示すパケット中継処理装置を構成する各部によって行われる処理を示すプログラムを用意する。そして、サーバ１１に備えられる各部によって行われる処理を示すプログラム（以下、サーバ１１用のプログラムという）をサーバ１１を実現すべきコンピュータ内のメモリ４２の特定のプログラムコードセグメントに格納する。

【０１８８】

また、ネットワーク接続装置２０に備えられる各部によって行われる処理を示すプログラム（以下、ネットワーク接続装置２０用のプログラムという）を、ネットワーク接続装置２０を実現すべきコンピュータ内のメモリ４２の特定のプログラムコードセグメントに格納する。ここで、ネットワーク接続装置２０を実現すべきコンピュータのＣＰＵは、例えば、ネットワークプロセッサである。なお、上述の各部によって行われる処理は、上記において、各フローチャートを用いて説明されている。

【０１８９】

入力装置４３は、例えば、キーボード、ポインティングデバイス、タッチパネル等であり、ユーザからの指示や情報の入力に用いられる。出力装置４４は、例えば、ディスプレイやプリンタ等であり、コンピュータ４０の利用者への問い合わせ、処理結果等の出力に用いられる。

【０１９０】

外部記憶装置４５は、例えば、磁気ディスク装置、光ディスク装置、光磁気ディスク装置等である。この外部記憶装置４５に上述のプログラムとデータを保存しておき、必要に応じて、それらをメモリ４２にロードして使用することもできる。

【０１９１】

媒体駆動装置４６は、可搬記録媒体４９を駆動し、その記録内容にアクセスする。可搬記録媒体４９としては、メモリカード、メモリスティック、フレキシブルディスク、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、光ディスク、

光磁気ディスク、ＤＶＤ（Digital Versatile Disk）等、任意のコンピュータで読み取り可能な記録媒体が用いられる。この可搬記録媒体４９に上述のプログラムとデータを格納しておき、必要に応じて、それらをメモリ４２にロードして使用することもできる。

【０１９２】

ネットワークインターフェース４７は、ＬＡＮ、ＷＡＮ等の任意のネットワーク（回線）を介して外部の装置を通信し、通信に伴なうデータ変換を行う。また、必要に応じて、上述のプログラムとデータを外部の装置から受け取り、それらをメモリ４２にロードして使用することもできる。

【０１９３】

図３７は、図３６のコンピュータにプログラムとデータを供給することができる、コンピュータで読み取り可能な記録媒体及び伝送信号を説明する図である。

記録媒体を用いて、上述のプログラムや各テーブルに格納されるデータを、サーバ１１を実現すべきコンピュータ及びネットワーク接続装置２０を実現すべきコンピュータに供給することにより、２以上のコンピュータにパケット中継処理装置に相当する機能を行なわせることも可能である。

【０１９４】

そのためには、上述のプログラムやデータを、コンピュータで読み取り可能な記録媒体４９に予め記憶させておく。そして、図３７に示すように、媒体駆動装置４６を用いて、記録媒体４９からサーバ１１用のプログラム等をサーバ１１を実現すべきコンピュータに読み出させて、そのコンピュータ（サーバ１１）のメモリ４２や外部記憶装置４５に一旦格納させ、そのコンピュータ（サーバ１１）の有するＣＰＵ４１にこの格納されたプログラムを読み出させて実行させる。

【０１９５】

同様に、記録媒体４９からネットワーク接続装置２０用のプログラム等をネットワーク接続装置２０を実現すべきコンピュータのメモリ４２等に一旦格納させ、そのコンピュータ（ネットワーク接続装置２０）の有するＣＰＵ４１に格納されたプログラムを読み出させて実行させる。

【０１９６】

また、記録媒体４９からプログラム等を、サーバ１１を実現すべきコンピュータ及びネットワーク接続装置２０を実現すべきコンピュータに読み出させる代わりに、プログラム（データ）提供者が有するＤＢ５０から、通信回線（ネットワーク）５１を介して、プログラムをそれぞれのコンピュータにダウンロードすることとしてもよい。この場合、例えば、ＤＢ５０を有しプログラムを送信するコンピュータでは、上記プログラムを表現するプログラム・データをプログラム・データ・シグナルに変換し、変換されたプログラム・データ・シグナルをモデムを用いて変調することにより伝送信号を得て、得られた伝送信号を通信回線５１（伝送媒体）に出力する。プログラムを受信するコンピュータでは、受信した伝送信号をモデムを用いて復調することにより、プログラム・データ・シグナルを得て、得られたプログラム・データ・シグナルを変換することにより、プログラム・データを得る。

【０１９７】

次に、図３８を用いて、サーバ１１を実現すべきコンピュータ及びネットワーク接続装置２０を実現すべきコンピュータへのプログラムやデータのローディングについて、例を挙げてより詳しく説明する。

【０１９８】

図３８に示すように、サーバ１１及びネットワーク接続装置２０を実現すべきコンピュータは、各々ＣＰＵ及びメモリを備え、上述の制御情報通信部３１を介して接続されている。また、例えば、制御情報通信部３１がＰＣＩバスである場合、ネットワーク接続装置２０をＰＣＩ用のＮＩＣ（Network Interface Card）として実現しても良い。

【０１９９】

例えば、サーバ１１用のプログラム等及びネットワーク接続装置２０用のプログラム等（ファームウェア）を記録した記録媒体がある場合、まず、サーバ１１を実現すべきコンピュータに備えられた不図示の媒体駆動装置を用いて記録媒体からサーバ１１用のプログラム等及びネットワーク接続装置２０用のプログラム等をサーバ１１のメモリにロードする（矢印Ａ４１）。続いて、サーバ１１のメモリに格納されたネットワーク接続装置２０用のプログラム等を、制御情報通信

部３１を介してネットワーク接続装置２０のメモリにロードする（矢印４２）。このようにして、サーバ１１を実現すべきコンピュータ及びネットワーク接続装置２０を実現すべきコンピュータに、それぞれに必要なプログラム等を供給することができる。サーバ１１のＣＰＵは、サーバ１１のメモリにロードされたサーバ１１用のプログラムを実行し、ネットワーク接続装置２０のＣＰＵは、ネットワーク接続装置２０のメモリにロードされたネットワーク接続装置２０用のプログラムを実行する。

【０２００】

また、上述のようにプログラム等を記録媒体からロードする代わりに、予めＲＯＭ等に記録しておくこととしても良い事は言うまでもない。また、記録媒体のかわりに伝送信号を用いてプログラム等をサーバ１１を実現すべきコンピュータに供給する事としても良い。

【０２０１】

また、ネットワーク接続装置２０において、ＣＰＵの代わりにＡＳＩＣ（Application Specific Integrated Circuit）を用いて、ネットワーク接続装置２０を構成する各部をハードウェアで構成する事としても良い。

【０２０２】

以上、本発明の実施形態について説明したが、本発明は上述した実施形態に限定されるものではなく、他の様々な変更が可能である。

（付記１）　ネットワーク接続装置を有するパケット中継処理装置であって、

上記ネットワーク接続装置がセッションを管理するセッション管理部と、

上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている

ことを特徴とするパケット中継処理装置。

（付記２）　上記ネットワーク接続装置は、更に、上記パケットのルーティング先に関するルーティング情報を格納するルーティングテーブルと、

上記セッションの開始時に、上記ルーティング情報に基づいて上記パケットのルーティング先を決定するルーティング処理部を更に備え、

上記パケット処理部は、上記パケットを上記ルーティング先に出力する、

ことを特徴とする付記１に記載のパケット中継処理装置。

（付記３）　上記パケット中継処理装置は、更に、サーバを備え、

上記サーバは、上記ルーティングテーブルに上記ルーティング情報を書き込むネットワーク制御部を備える、

ことを特徴とする付記１に記載のパケット中継処理装置。

（付記４）　上記パケット中継処理装置は、さらに、サーバを備え、

上記サーバは、上記セッションを管理する外部セッション管理部を備え、

上記セッション管理部は、与えられた条件に応じて上記セッションに関するセッション情報を上記サーバに転送し、

上記外部セッション管理部は、受信した上記セッション情報に基づいて上記セッションを管理する、

ことを特徴とする付記１に記載のパケット中継処理装置。

（付記５）　上記ネットワーク接続装置は、更に処理振分部と複数のサービス処理部を備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも１つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする付記１に記載のパケット中継処理装置。

（付記６）　上記パケット中継処理装置は、更にサーバを備え、

上記サーバは、外部サービス処理部を備え、

上記処理振分部は、与えられた条件によって、上記パケットを上記サーバに転送し、

上記外部サービス処理部は、受信したパケットに対するサービスを実行する、

ことを特徴とする付記５のパケット中継処理装置。

（付記７）　上記パケット中継処理装置は、サーバを更に備え、

上記サーバは、パケット詳細解析部を備え、

上記ネットワーク接続装置は、更に処理振分部とサービス処理部を備え、

上記処理振分部が、与えられた条件によって上記パケットを上記パケット詳細

解析部に転送し、

上記パケット詳細解析部は、上記パケットを解析することにより上記パケットに対するサービス内容を決定し、決定した上記サービス内容を上記ネットワーク接続装置に設定し、

上記設定後、上記ネットワーク接続装置は、上記決定されたサービス内容に基づいて上記パケットを処理する、

ことを特徴とする付記１に記載のパケット中継処理装置。

（付記８）　上記サービス処理部として、上記パケットのヘッダを書き換える機能を持つことを特徴とする付記５に記載のパケット中継処理装置。

（付記９）　上記サービス処理部として、パケットを廃棄する機能を持つことを特徴とする付記５に記載のパケット中継処理装置。

（付記１０）　上記サービス処理部は、上記サーバの負荷分散のために、負荷の振分先を決定する機能を持つことを特徴とする付記５に記載のパケット中継処理装置。

（付記１１）　上記ネットワーク接続装置は、上記セッションに関するセッション情報を格納するセッションテーブルと、上記パケットに対するサービスを実行するための規則を記述するポリシーを格納するポリシーテーブルを備え、

上記セッション管理部は、上記パケットを受信した場合、上記パケットに含まれる情報を検索キーとして用いてセッションテーブルを検索し、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されていない場合には、上記セッション管理部は、さらに上記パケットに含まれる情報を検索キーに基づいて、上記ポリシーテーブルから上記ポリシーを取得し、上記取得したポリシーに基づいて、上記セッション情報を上記セッションテーブルに書き込み、

上記検索の結果、該当するセッション情報が上記セッションテーブルに登録されている場合には、上記セッション管理部は、上記セッションの状態に基づいて、上記セッションテーブルに格納されたセッション情報を管理することを特徴とする付記５に記載のパケット中継処理装置。

（付記１２）　上記パケット中継処理装置はサーバを備え、

上記サーバは、上記ポリシーを上記ポリシーテーブルに書き込むサービス制御部を備える、

ことを特徴とする付記１１に記載のパケット中継処理装置。

（付記１３）　上記セッションテーブルを検索する際の上記検索キーが、ＩＰパケットの宛先及び送信元ＩＰアドレス、プロトコル、宛先及び送信元ポート番号、入力インタフェースを含むことを特徴とする付記１１に記載のパケット中継処理装置。

（付記１４）上記セッションテーブルが、上記検索キー、上記セッションの状態、適用サービス及び上記適用サービスに固有な情報をエントリとしてを持つことを特徴とする付記１１に記載のパケット中継処理装置。

（付記１５）　上記ポリシーテーブルが、ＩＰパケットの宛先及び送信元ＩＰアドレス、プロトコル、宛先及び送信元ポート番号、適用サービスと上記適用サービスに固有な情報、優先度をエントリとして持つことを特徴とする付記１１に記載のパケット中継処理装置。

（付記１６）　上記セッション管理部は、更に、上記セッションが終了してから所定時間経過した後に、上記終了したセッションに関するセッション情報を上記セッションテーブルから削除することを特徴とする付記１に記載のパケット中継処理装置。

（付記１７）　上記ネットワーク接続装置は、更に、パケットに関する統計情報を取得するためのカウンタを備えることを特徴とする付記１に記載のパケット中継処理装置。

（付記１８）　複数のポリシーは複数のグループに分けられ、

上記ネットワーク接続装置は、更に、上記グループ毎に各ポリシーが有効であるか否かを設定することを特徴とする付記１１に記載のパケット中継処理装置。

（付記１９）　上記ネットワーク接続装置は、更に、上記パケットのログを採取するために、上記パケットの少なくとも一部を上記サーバに転送することを特徴とする付記１２に記載のパケット中継処理装置。

（付記２０）　上記パケットの一部は、上記パケットのヘッダであることを特徴とする付記１８に記載のパケット中継処理装置。

（付記２１）　上記セッション情報は、上記サーバに上記パケットを転送するべきか否かを示すサーバ転送指示情報を含み、上記処理振分部は、上記サーバ転送指示情報に基づいて、上記パケットを上記サーバへの転送を行うか否かを決定する事を特徴とする付記１２に記載のパケット中継処理装置。

（付記２２）　上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがＨＴＴＰプロトコルのＧＥＴパケットである場合、上記パケットに含まれるＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）に基づいて、上記パケットに対するサービスを決定する、

ことを特徴とする付記７に記載のパケット中継処理装置。

（付記２３）　上記パケット詳細解析部は、更に、上記サーバに転送された上記パケットがＦＴＰプロトコルのＰＯＲＴ命令、或いはＰＡＳＶ命令のＡＣＫである場合、上記セッションのデータコネクションのＩＰアドレスとポート番号に基づいて、上記パケットに対するサービスを決定する、

ことを特徴とする付記７に記載のパケット中継処理装置。

（付記２４）　上記パケット詳細解析部は、上記サーバの負荷を分散させる処理を行う場合、上記負荷の振分先となる振分先サーバが決定されるまで、上記振分先サーバに代わって応答することを特徴とする付記７に記載のパケット中継処理装置。

（付記２５）　上記パケット詳細解析部は、上記パケットを解析することにより、上記セッションテーブルに、上記パケットに対するサービスの種類、変換用ＩＰアドレス及びポート番号、シーケンス番号及びＡＣＫ番号差分を書き込む、

ことを特徴とする付記２１に記載のパケット中継処理装置。

（付記２６）　パケット中継処理装置におけるネットワーク接続装置であって、

上記ネットワーク接続装置がセッションを管理するセッション管理部と、

上記セッション管理部によるセッション管理に基づいてパケットを中継するパケット処理部を備えている

ことを特徴とするネットワーク接続装置。

（付記２７）　上記ネットワーク接続装置は、与えられた条件に応じて上記セッションに関するセッション情報を上記パケット中継処理装置に備えられたサーバ

に転送するサーバ転送部を備え、

上記サーバは転送された上記セッション情報により上記セッションの管理を行う

ことを特徴とする付記２６のネットワーク接続装置。

（付記２８）　上記ネットワーク接続装置は処理振分部と複数のサービス処理部を更に備え、

上記処理振分部は、上記パケットに対するサービスの内容に基づいて、上記複数のサービス処理部のうち少なくとも１つに上記パケットを振り分け、

上記パケットを振り分けられたサービス処理部は、上記パケットに対するサービス処理を実行する、

ことを特徴とする付記２６のネットワーク接続装置。

（付記２９）　上記処理振分部は、与えられた条件によって、上記パケットを上記パケット中継処理装置に備えられたサーバに転送し、上記サーバに上記パケットに対するサービス処理を実行させる

ことを特徴とする付記２６のネットワーク接続装置。

（付記３０）　上記ネットワーク接続装置が処理振分部とサービス処理部を更に備え、

上記処理振分部は、与えられた条件によって上記パケットをパケット中継処理装置に備えられたサーバに、上記パケットに対するサービスを決定するために転送し、

上記サービス処理部は、上記サーバによるサービスの決定以後、上記サーバで決定したサービス内容に基づいて上記セッションのパケットを処理する

ことを特徴とする付記２６のネットワーク接続装置。

（付記３１）　パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムであって、

セッションを管理し、

上記セッション管理に基づいて上記パケットを中継する

ことを含む処理を上記コンピュータに実行させることを特徴とするプログラム。

（付記３２）　与えられた条件に応じて上記セッションに関するセッション情報を上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記セッションの管理を行わせるために転送する、
ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記３１に記載のプログラム。
（付記３３）　上記パケットに対するサービスの内容に基づいて、上記サービスに対応する処理を行う装置又はプログラムセグメントに、上記パケットを振り分ける、
ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記３１に記載のプログラム。
（付記３４）　与えられた条件に応じて上記パケットを上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記パケットに対するサービスを実行させるために転送する、
ことを更に含む処理を上記コンピュータに実行させることを特徴とする付記３３に記載のプログラム。
（付記３５）　与えられた条件に応じて、上記ネットワーク接続装置に接続されたサーバへ、上記パケットに対するサービスを決定するために上記パケットを転送し、
　上記サーバによる上記パケットに対するサービスの決定以後、上記決定されたサービス内容に基づきパケットを処理する
ことを含む処理を上記コンピュータに実行させること特徴とする付記３１に記載のプログラム。
（付記３６）　パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムであって、
　上記ネットワーク接続装置が上記パケットを処理するために、上記パケットに対するサービスを実行するための規則を記述するポリシーを上記ネットワーク接続装置に設定する、
ことを含む処理を上記サーバに実行させることを特徴とするプログラム。
（付記３７）　上記ネットワーク接続装置から転送された上記パケットを受信し

、受信した上記パケットに対するサービスを実行する、
ことを含む処理を上記サーバに実行させることを特徴とする付記３６に記載のプログラム。
（付記３８）　パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムであって、
上記ネットワーク接続装置から転送された上記パケットを受信し、
上記パケットを解析することにより、上記パケットに対するサービスの内容を決定し、
上記決定されたサービス内容に基づいて上記ネットワーク接続装置に上記パケットを処理させるために、該決定されたサービスの内容を上記ネットワーク接続装置に設定する、
ことを含む処理を上記サーバに実行させることを特徴とするプログラム。
（付記３９）　パケットを中継する制御を、ネットワーク接続装置に備えられたコンピュータに実行させるプログラムを記録した記録媒体であって、
セッションを管理し、
上記セッション管理に基づいて上記パケットを中継する
ことを含む処理を上記コンピュータに実行させるプログラムを記録した記録媒体。
（付記４０）　与えられた条件に応じて上記セッションに関するセッション情報を上記ネットワーク接続装置に接続されたサーバに、上記サーバに上記セッションの管理を行わせるために転送する、
ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記３９に記載の記録媒体。
（付記４１）　上記パケットに対するサービスの内容に基づいて、上記サービスに対応する処理を行う装置又はプログラムセグメントに、上記パケットを振り分ける、
ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記３９に記載の記録媒体。
（付記４２）　与えられた条件に応じて上記パケットを上記ネットワーク接続

装置に接続されたサーバに、上記サーバに上記パケットに対するサービスを実行させるために転送する、

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記３９に記載の記録媒体。

（付記４３）　与えられた条件に応じて、上記ネットワーク接続装置に接続されたサーバへ、上記パケットに対するサービスを決定するために上記パケットを転送し、

上記サーバによる上記パケットに対するサービスの決定以後、上記決定されたサービス内容に基づきパケットを処理する

ことを更に含む処理を上記コンピュータに実行させるプログラムを記録した付記３９に記載の記録媒体。

（付記４４）　パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムを記録した記録媒体であって、

上記ネットワーク接続装置が上記パケットを処理するために、上記パケットに対するサービスを実行するための規則を記述するポリシーを上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させるプログラムを記録した記録媒体。

（付記４５）　上記ネットワーク接続装置から転送された上記パケットを受信し、受信した上記パケットに対するサービスを実行する、

ことを更に含む処理を上記サーバに実行させるプログラムを記録した付記４４に記載の記録媒体。

（付記４６）　パケットを中継する機能を有するネットワーク接続装置に接続されたサーバに実行させるプログラムを記録した記録媒体であって、

上記ネットワーク接続装置から転送された上記パケットを受信し、

上記パケットを解析することにより、上記パケットに対するサービスの内容を決定し、

上記決定されたサービス内容に基づいて上記ネットワーク接続装置に上記パケットを処理させるために、該決定されたサービスの内容を上記ネットワーク接続装置に設定する、

ことを含む処理を上記サーバに実行させるプログラムを記録した記録媒体。

【０２０３】

【発明の効果】

以上説明したように、本発明においては、以下の効果を得ることができる。

（１）上記ネットワーク接続装置にセッション管理に基づくパケット中継処理部を設け、ネットワーク接続装置により、セッション管理に基づく中継処理を行うようにする。これにより、サーバのＣＰＵ使用率を下げることができる。また、ネットワーク接続装置上でセッション管理を行い、セッション開始時にセッションテーブルに出力先を登録することにより、セッションの途中でルーティングテーブルが変更されても、現在継続中のセッションについては、一貫性を保持できる。

（２）パケット中継処理装置のサーバに外部セッション管理機能を設け、ネットワーク接続装置からセッション情報を上記サーバに転送し、サーバによりセッション管理を行うことにより、セッション数がネットワーク接続装置のセッションテーブル登録数を上回った場合でも、ネットワーク接続装置で溢れた分をサーバで管理することができる。

〈３〉処理振分部と複数のサービス処理部をサーバに比べ高速に処理できるネットワーク接続装置に配置することにより、サーバのＣＰＵの使用率を小さくすることができるとともに、サービス処理を高速化することができる。

（４）サーバに外部サービス処理部を設け、サービス処理を、ネットワーク接続装置とサーバの両方で実行できるようにすることにより、ネットワーク接続装置２上で実現するのは困難なサービス処理をサーバで行うことができ、ネットワーク接続装置が上記決定されたサービス内容に基づき中継処理を行うようにすることにより、サーバで全ての処理を行う場合に比べ、サービス処理を高速に実現することが可能となる。

【図面の簡単な説明】

【図１】

本発明の概要を説明する図である。

【図２】

本発明の第１の実施例のパケット中継処理装置の構成を示す図である。

【図３】

転送パケットのフレーム構成を示す図である。

【図４】

パケット処理部の処理フローを示す図である。

【図５】

セッション管理部の処理フローを示す図である。

【図６】

セッションテーブルの構成例を示す図である。

【図７】

ＴＣＰの状態遷移を示す図である。

【図８】

ＴＣＰのセッション開始からセッション終了までの状態遷移を説明する図である。

【図９】

ＵＤＰの状態遷移を示す図である。

【図１０】

本発明の第２の実施例のパケット中継処理装置の構成を示す図である。

【図１１】

第２の実施例のセッション管理部、外部セッション管理部における処理フローを示す図である。

【図１２】

本発明の第３の実施例のパケット中継処理装置の構成を示す図である。

【図１３】

第３実施例に係わるセッションテーブルの構成例を示す図である。

【図１４】

第３実施例にかかわるポリシーテーブルの構成例を示す図である。

【図１５】

本発明の第３の実施例のセッション管理部の処理フローを示す図である。

【図１６】

第３の実施例の処理振分部及びサービス処理部における処理フローを示す図である。

【図１７】

第３実施例におけるポリシー検索終了後の負荷分散サービスでのパケットフローを示す図である。

【図１８】

本発明の第４の実施例のパケット中継処理装置の構成を示す図である。

【図１９】

第４の実施例に係わる処理振分部、サービス処理部及び外部サービス処理部における処理の手順を示すフローチャートである。

【図２０】

本発明の第５の実施例のパケット中継処理装置の構成を示す図である。

【図２１】

第５実施例に係わるセッションテーブルの一例を示す図（その１）である。

【図２２】

第５実施例に係わるセッションテーブルの一例を示す図（その２）である。

【図２３】

第５実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その１）である。

【図２４】

第５実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その２）である。

【図２５】

詳細解析用セッションテーブルの構成例を示す図である。

【図２６】

詳細解析用ポリシーテーブルの構成例を示す図である。

【図２７】

第５実施例に係わるパケット中継処理装置の動作概念を示す図である。

【図２８】

第５の実施例に係わる処理振分部、サービス処理部及びパケット詳細解析部における処理の手順を示すフローチャートである。

【図２９】

パケット詳細解析部における処理の手順を示すフローチャートである。

【図３０】

ＵＲＬフィルタリングの動作を説明する図である。

【図３１】

ＵＲＬ負荷分散サービスの動作を説明する図である。

【図３２】

ＦＴＰフィルタリングの動作を説明する図である。

【図３３】

第５実施例における詳細解析前のＵＲＬ負荷分散サービスでのパケットフローを示す図である。

【図３４】

第５実施例における詳細解析後のＵＲＬ負荷分散サービスでのパケットフローを示す図である。

【図３５】

フラグテーブルのデータ構造の一例を示す図である。

【図３６】

コンピュータの構成図である。

【図３７】

コンピュータにプログラムやデータを供給する記録媒体や伝送信号を説明する図である。

【図３８】

サーバ及びネットワーク接続装置へのプログラムやデータのローディングを説明する図である。

【図３９】

従来のパケット中継処理装置の構成を示す図である。

【符合の説明】

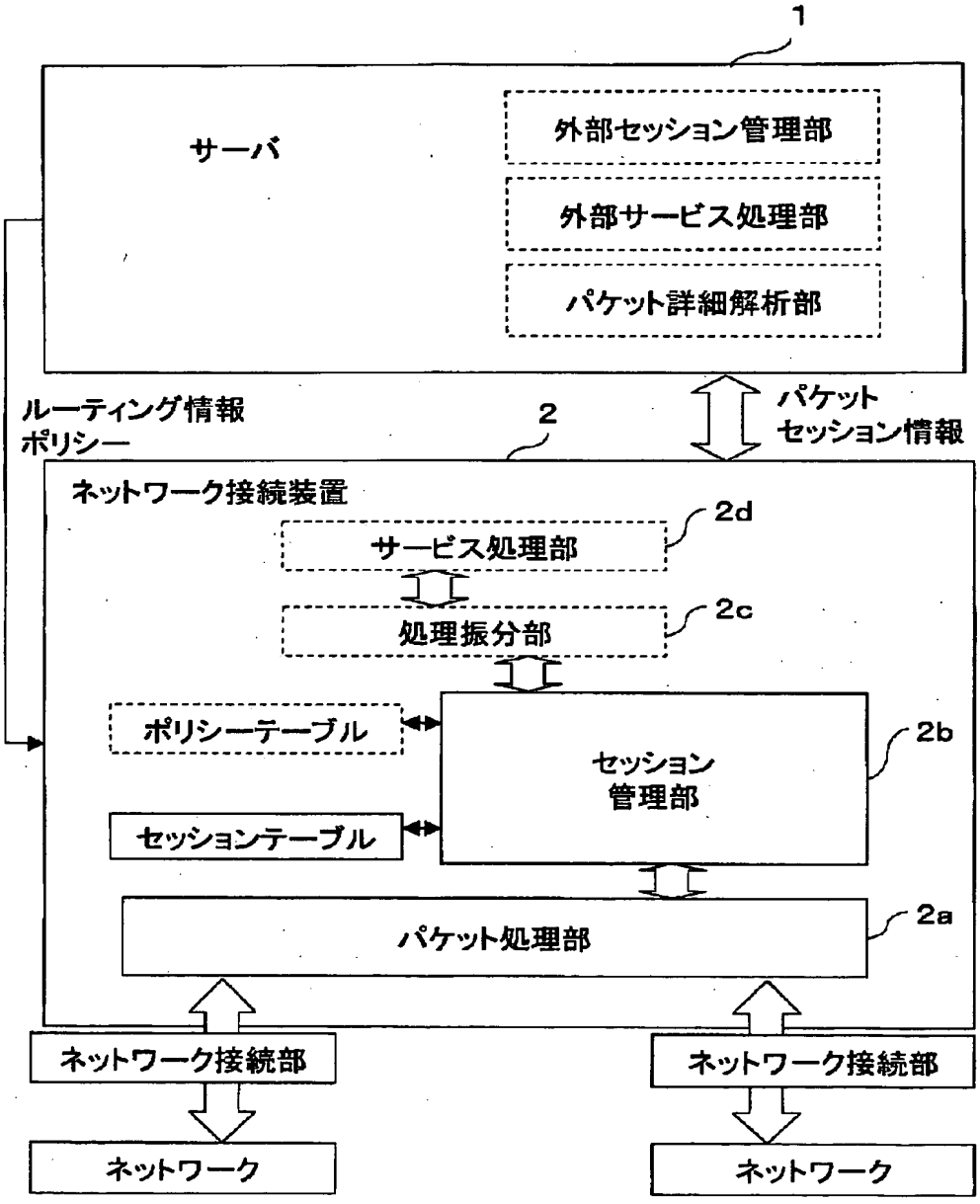
１　サーバ
２　ネットワーク接続装置
１１　サーバ
１２　ネットワーク制御部
１３　外部セッション管理部
１３ａ　外部セッションテーブル
１４　サービス制御部
１５　外部サービス処理部
１６　パケット詳細解析部
２０　ネットワーク接続装置
２１　パケット処理部
２２　セッション管理部
２２ａ　セッションテーブル
２２ａ’　セッションテーブル
２３　ルーティング処理部
２３ａ　ルーティングテーブル
２４　サーバ転送部
２５　ポリシーテーブル
２６　処理振分部
２７　サービス処理部
３０　ネットワーク接続部
３１　制御情報通信部
３２　セッション情報通信部
３３　パケット通信路
４０　コンピュータ
４１　ＣＰＵ
４２　メモリ

４３　入力装置
４４　出力装置
４５　外部記憶装置
４６　媒体駆動装置
４７　ネットワークインターフェース
４８　バス
４９　可搬記録媒体
５０　データベース
５１　回線
Ａ　矢印
Ｐ　パケット
Ｓ　ステップ

【書類名】　図面

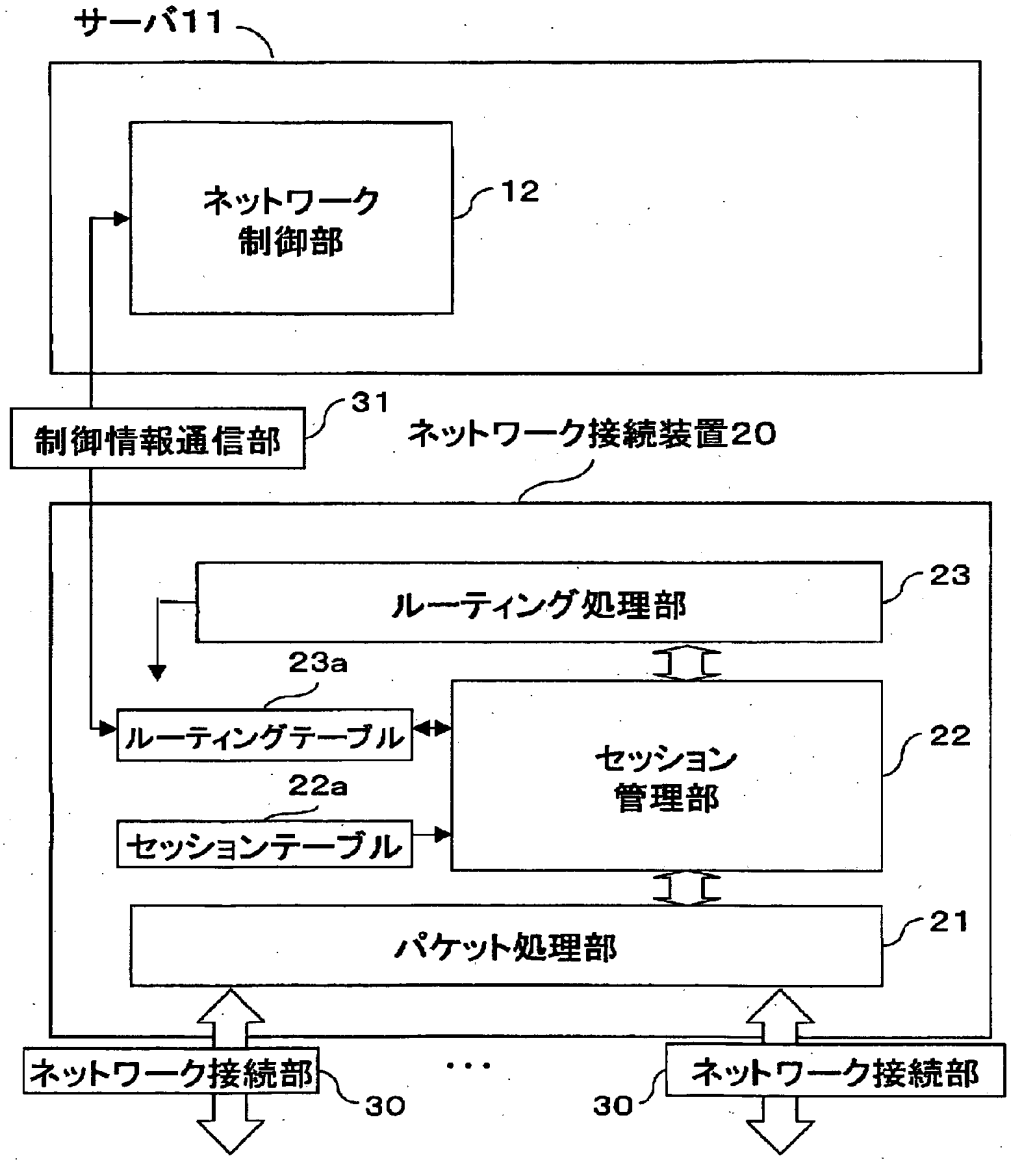
【図１】

本発明の概要を示す図



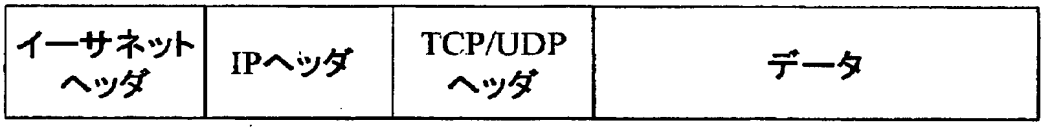
【図２】

本発明の第1の実施例のパケット中継処理装置の構成を示す図



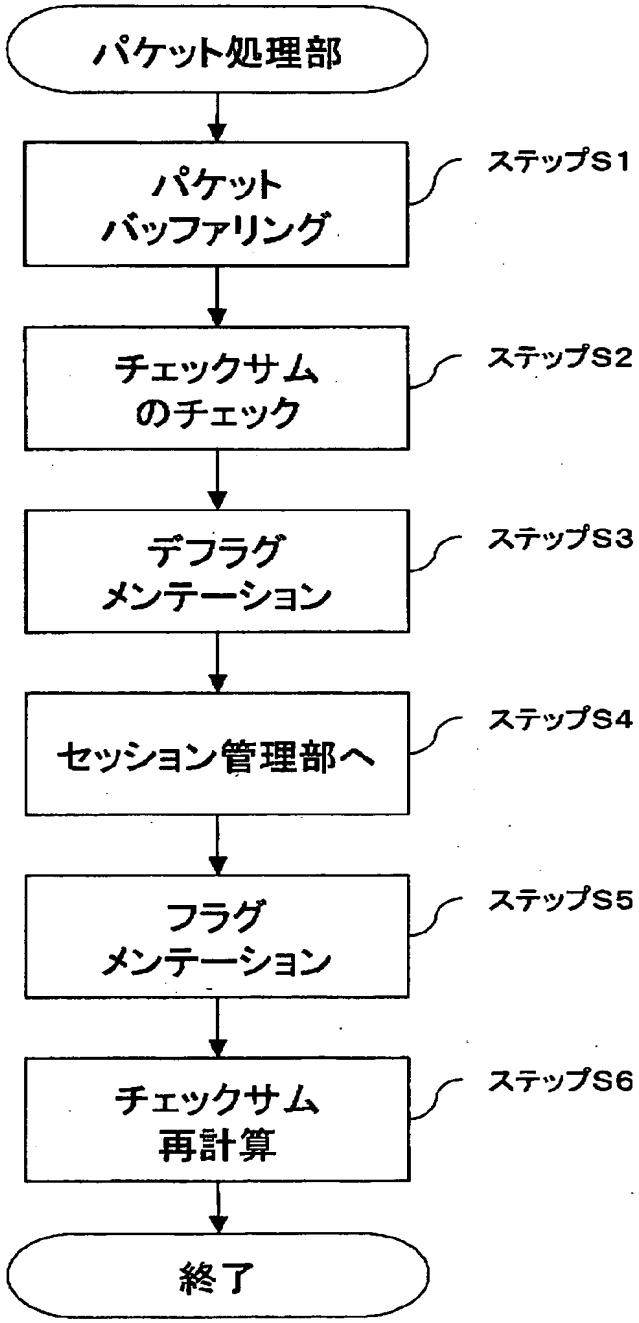
【図３】

転送パケットのフレーム構成を示す図



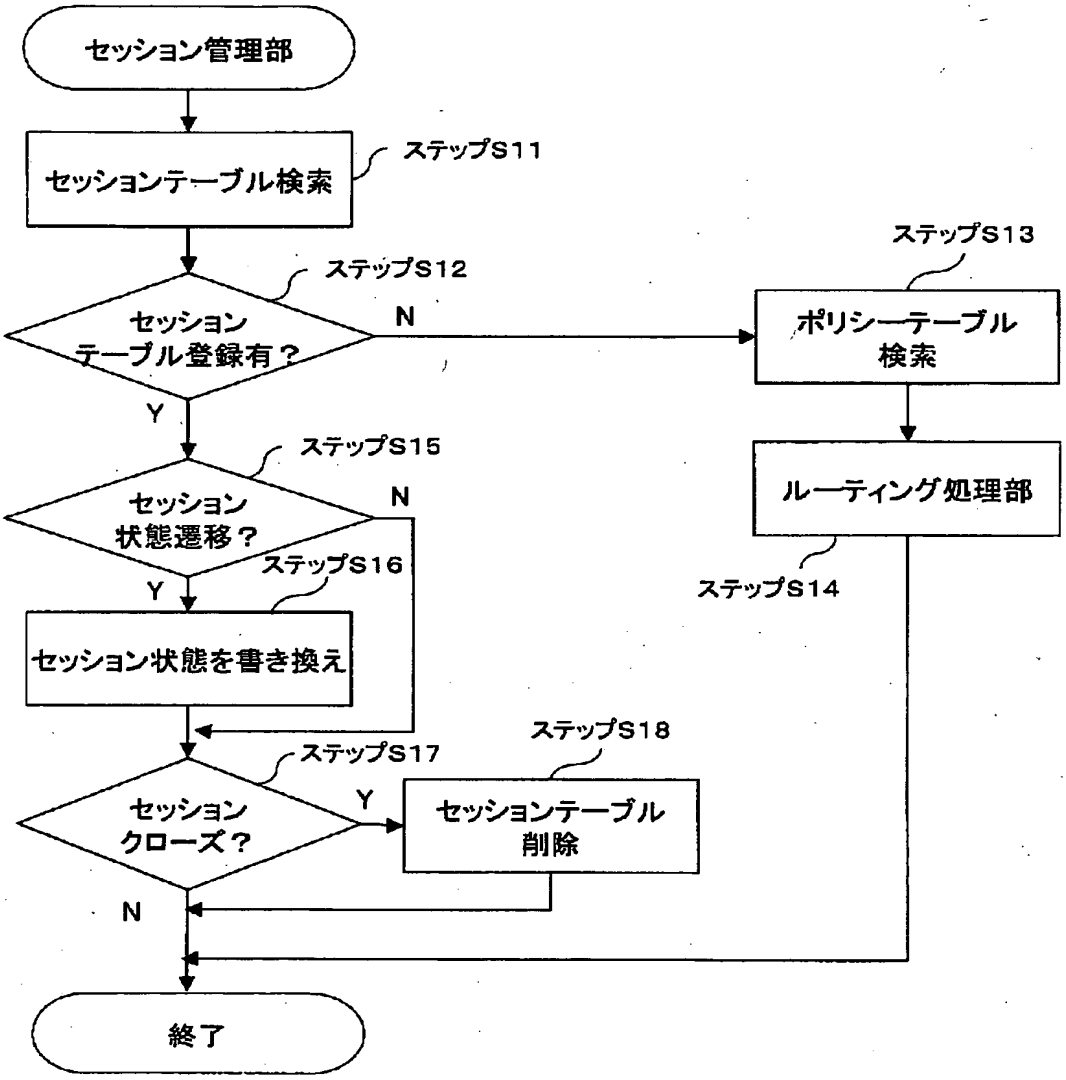
【図４】

パケット処理部の処理フローを示す図



【図５】

セッション管理部の処理フローを示す図



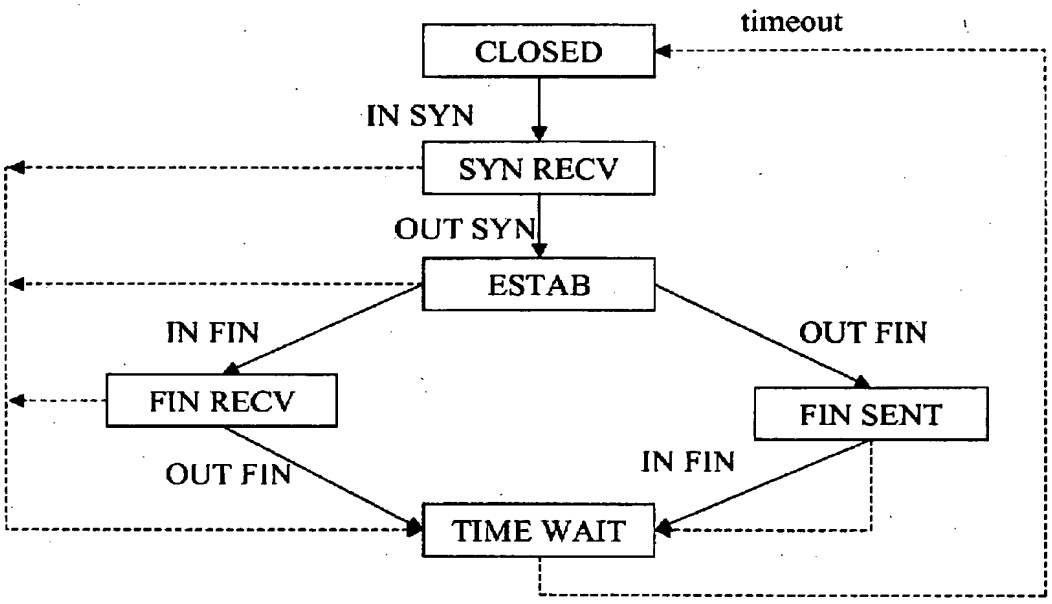
【図６】

セッションテーブルの構成例を示す図

セッションID	セッション検索キー						
	送信元IPアドレス	送信元ポート番号	プロトコル	宛先IPアドレス	宛先ポート番号	セッション状態	出力先
0	192.168.100.14	13200	TCP	192.168.10.5	8080	ESTAB	
1	192.168.10.5	8080	TCP	192.168.100.14	13200	ESTAB	
2	192.168.100.100	http	TCP	10.25.1.230	9250	IN SYN	
3	10.25.1.230	9250	TCP	192.168.100.75	http	IN SYN	

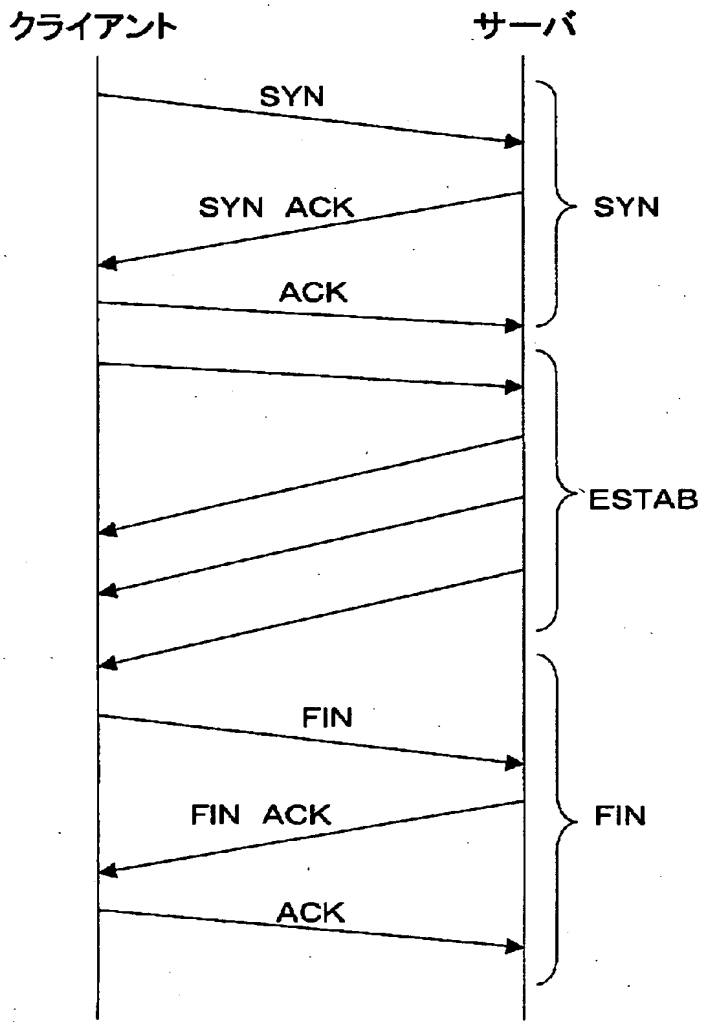
【図７】

TCPの状態遷移を示す図



【図８】

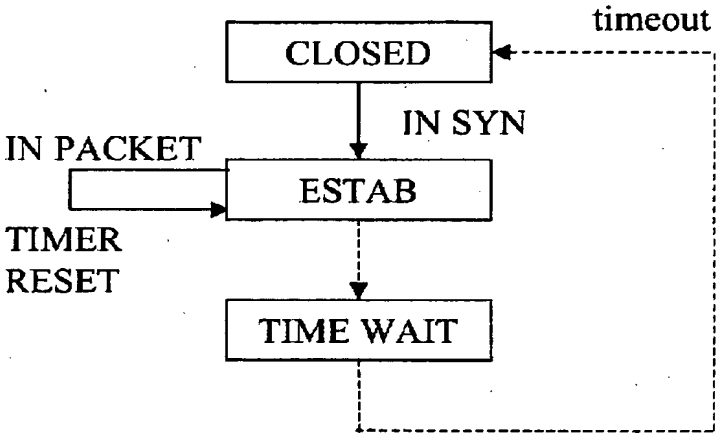
TCPのセッション開始から終了までの状態遷移を説明する図



【図９】

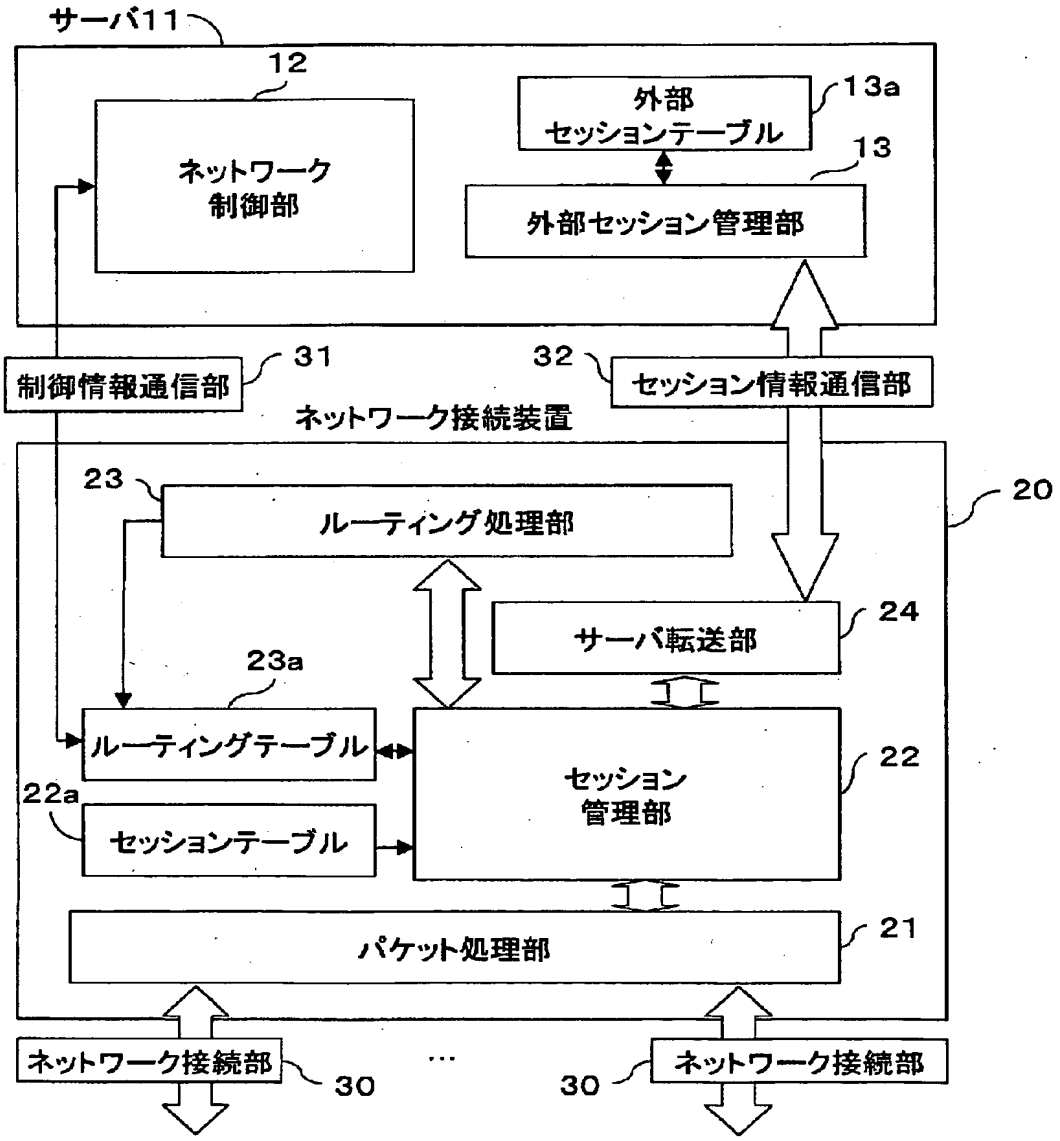
UDPの状態遷移を示す図

（UDP）



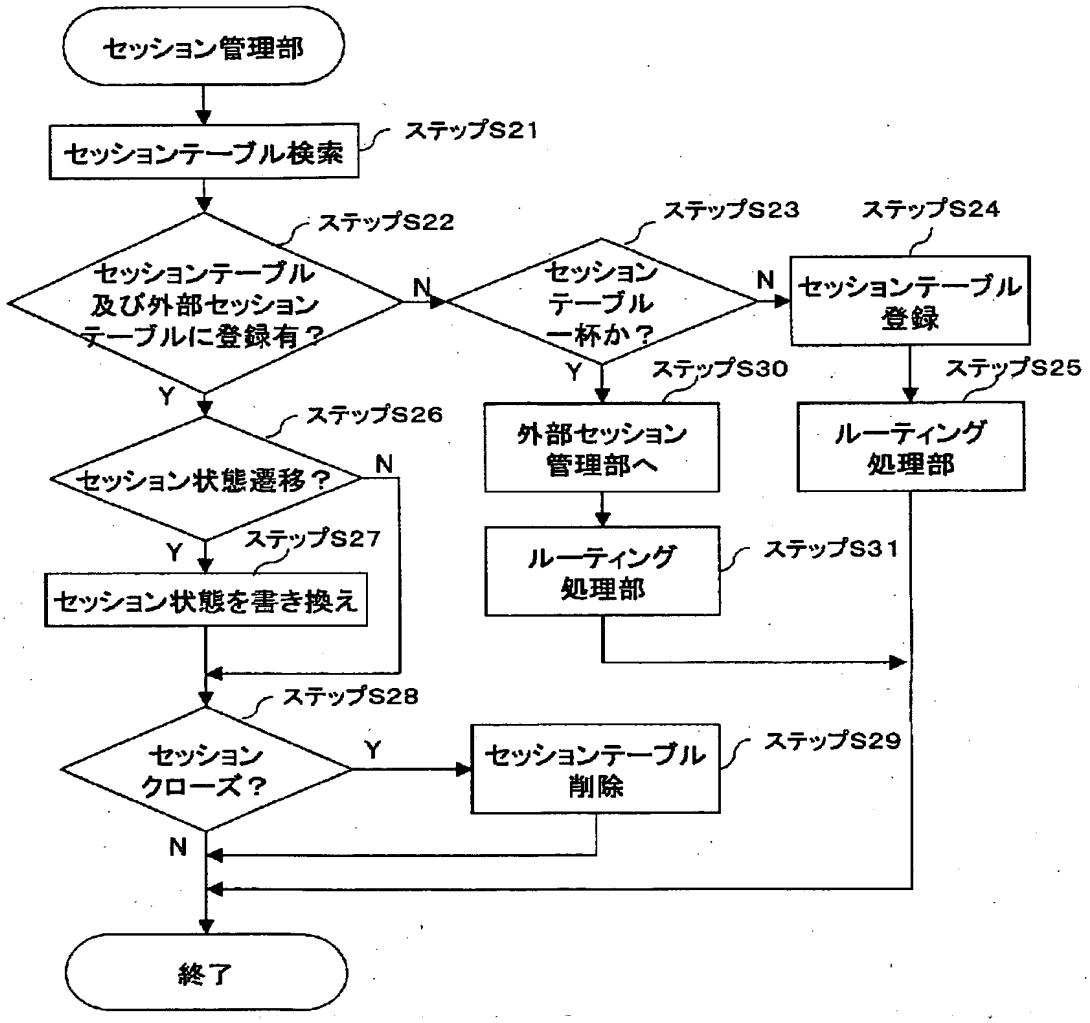
【図１０】

本発明の第2の実施例のパケット中継処理装置の構成を示す図



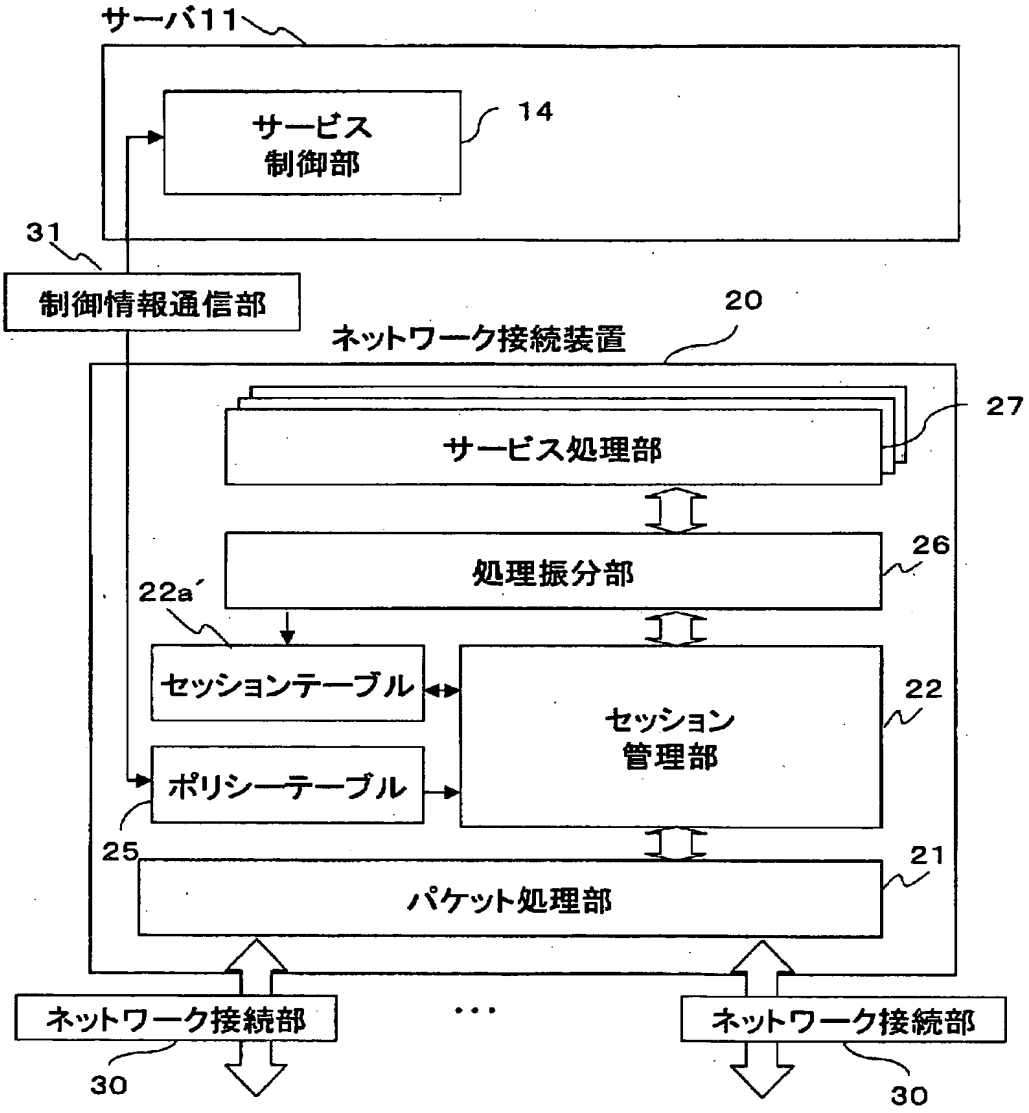
【図１１】

第2の実施例のセッション管理部、
外部セッション管理部における処理フローを示す図



【図１２】

本発明の第3の実施例のパケット中継処理装置の構成を示す図



【図１３】

第3実施例に係るセッションテーブルの構成例を示す図

セッションＩＤ		0	1	2	3
セッション検索キー	送信元ＩＰアドレス	192.168.100.14	192.168.10.5	192.168.100.100	10.25.1.230
	送信元ポート番号	13200	8080	http	9250
	プロトコル	TCP	TCP	TCP	TCP
	宛先ＩＰアドレス	192.168.10.5	192.168.100.14	10.25.1.230	192.168.100.75
	宛先ポート番号	8080	13200	9250	http
	入力インタフェース	0	1	0	1
セッション状態		ESTAB	ESTAB	IN SYN	IN SYN
出力先インタフェース		1	0	1	0
適用サービスタイプ		ﾌｨﾙﾀﾘﾝｸﾞ通過	ﾌｨﾙﾀﾘﾝｸﾞ通過	ヘッダ書換	ヘッダ書換
固有情報		-	-	Src:192.168.100.75	Dst:192.168.100.100
一貫性保持時間(ms)		1000	1000	3000	3000
イベントフラグ(パケット)		OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)		ON	ON	OFF	OFF

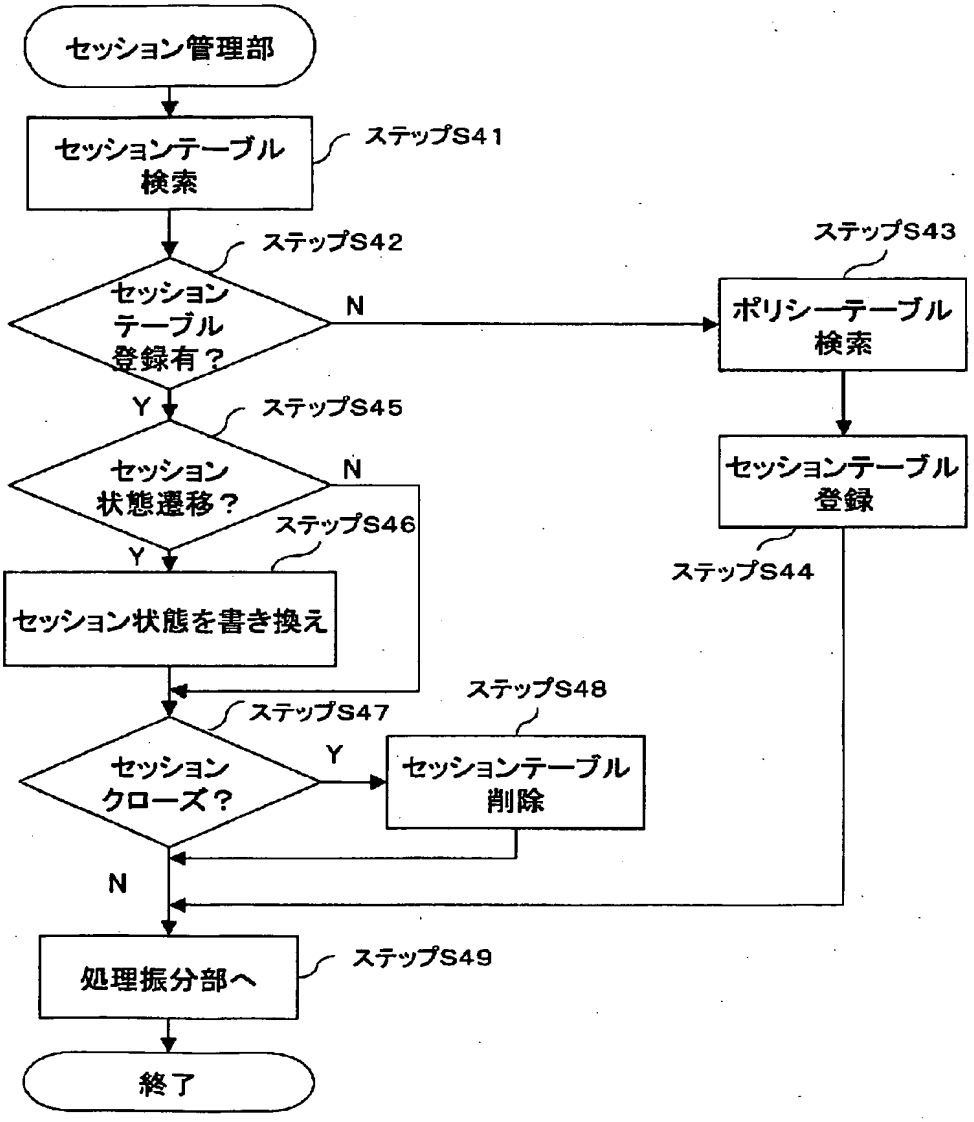
【図１４】

第3実施例に係るポリシーテーブルの構成例を示す図

ポリシーＩＤ		0	1
ポリシー検索キー	送信元ＩＰアドレス	Any	Any
	送信元ポート番号	Any	Any
	プロトコル	Any	TCP
	宛先ＩＰアドレス	GW	192.168.100.75
	宛先ポート番号	Any	http
適用サービスタイプ		ﾌｨﾙﾀﾘﾝｸﾞ廃棄	負荷分散
サービス固有情報		-	振り分け先1: 192.168.100.100 振り分け先2: 192.168.100.110 振り分け先3: 192.168.100.120 振り分け先4: 192.168.100.130 振り分け方法: ラウンドロビン
優先度		5000	1000
グループID		6	32
イベントフラグ(パケット)		OFF	OFF
イベントフラグ(ヘッダ)		ON	OFF
一貫性保持時間（ms）		1000	3000
ポリシーヒット数		2	2

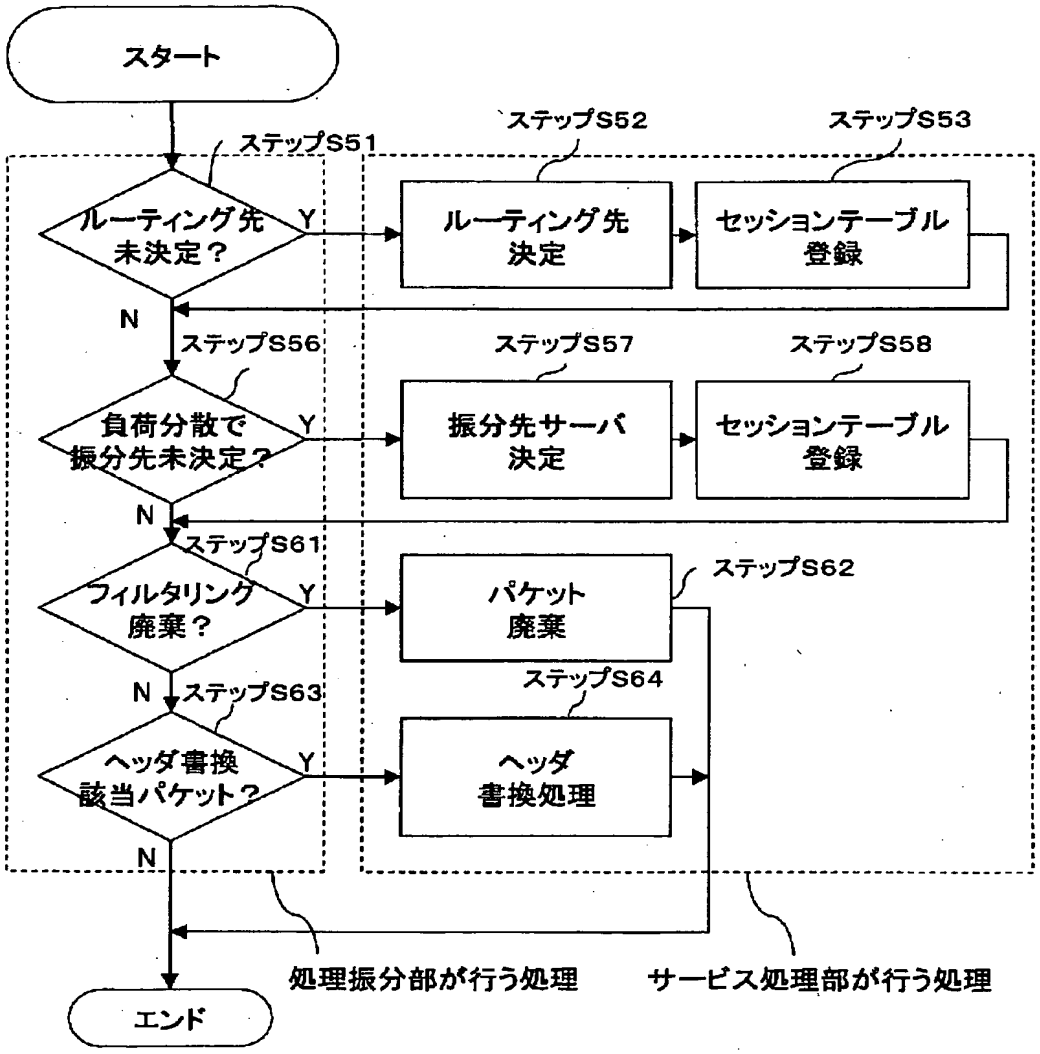
【図１５】

本発明の第3の実施例のセッション管理部の処理フローを示す図



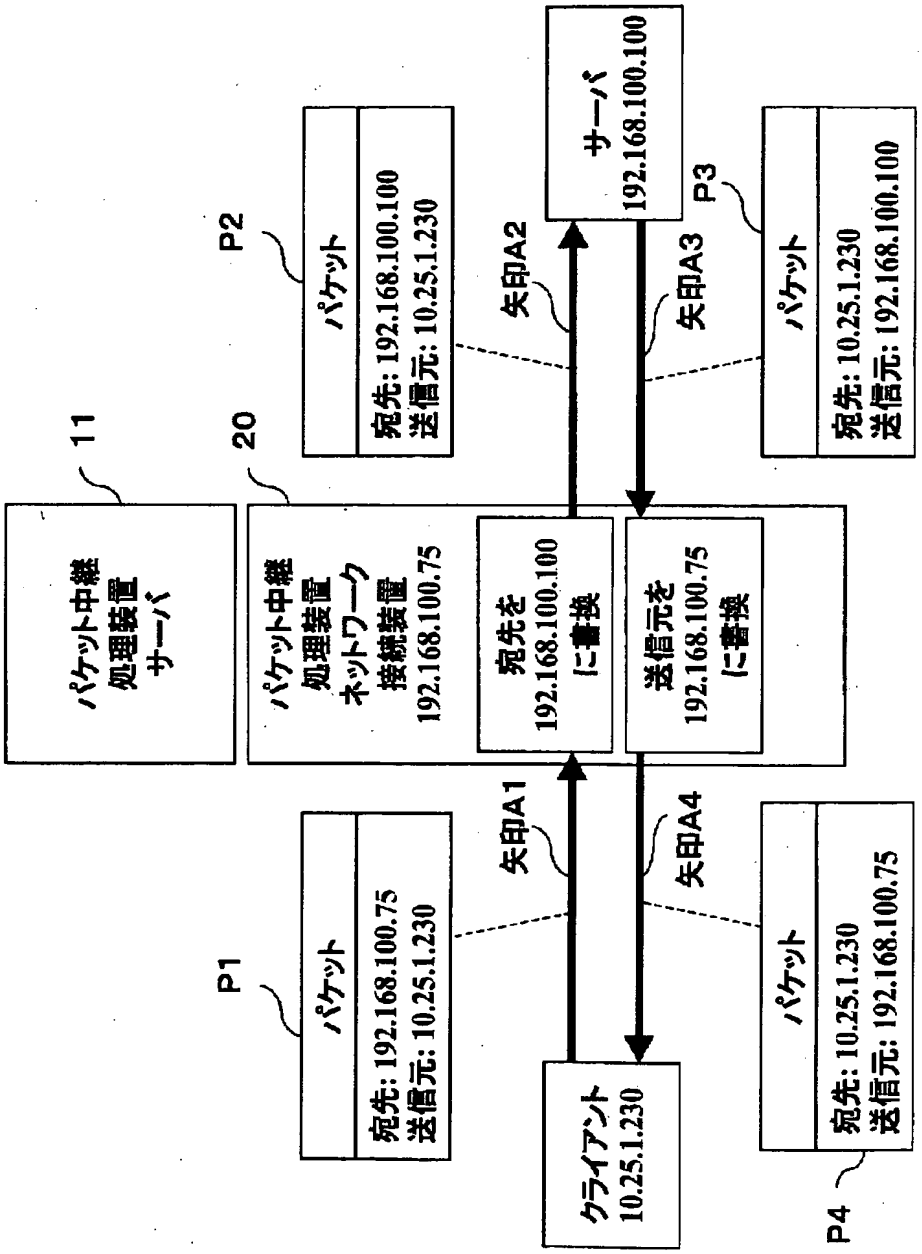
【図１６】

第3実施例に係る処理振分部及び
サービス処理部の処理フローを示す図



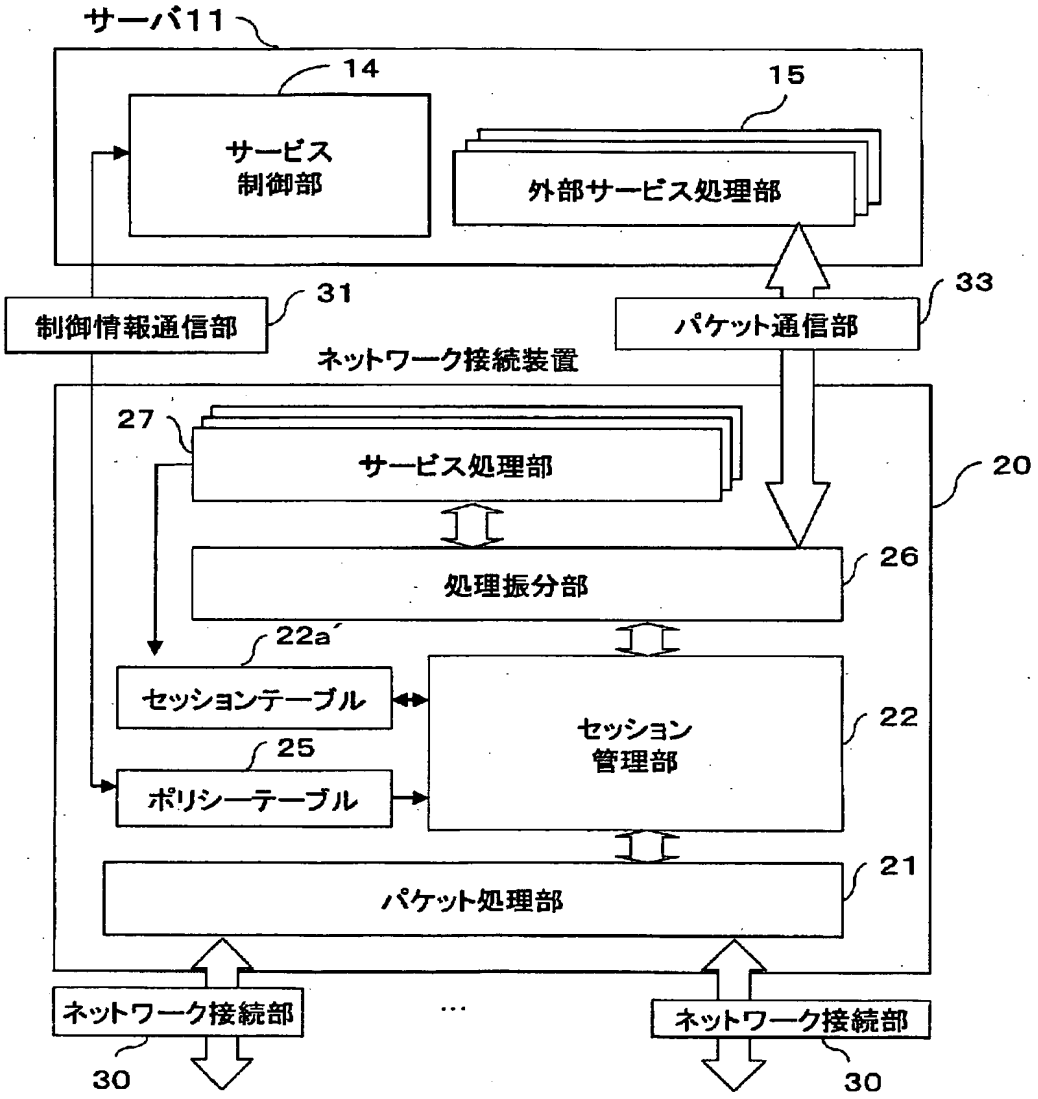
【図１７】

第3実施例における負荷分散サービスの
パケットフローを示す図(ポリシー検索終了後)



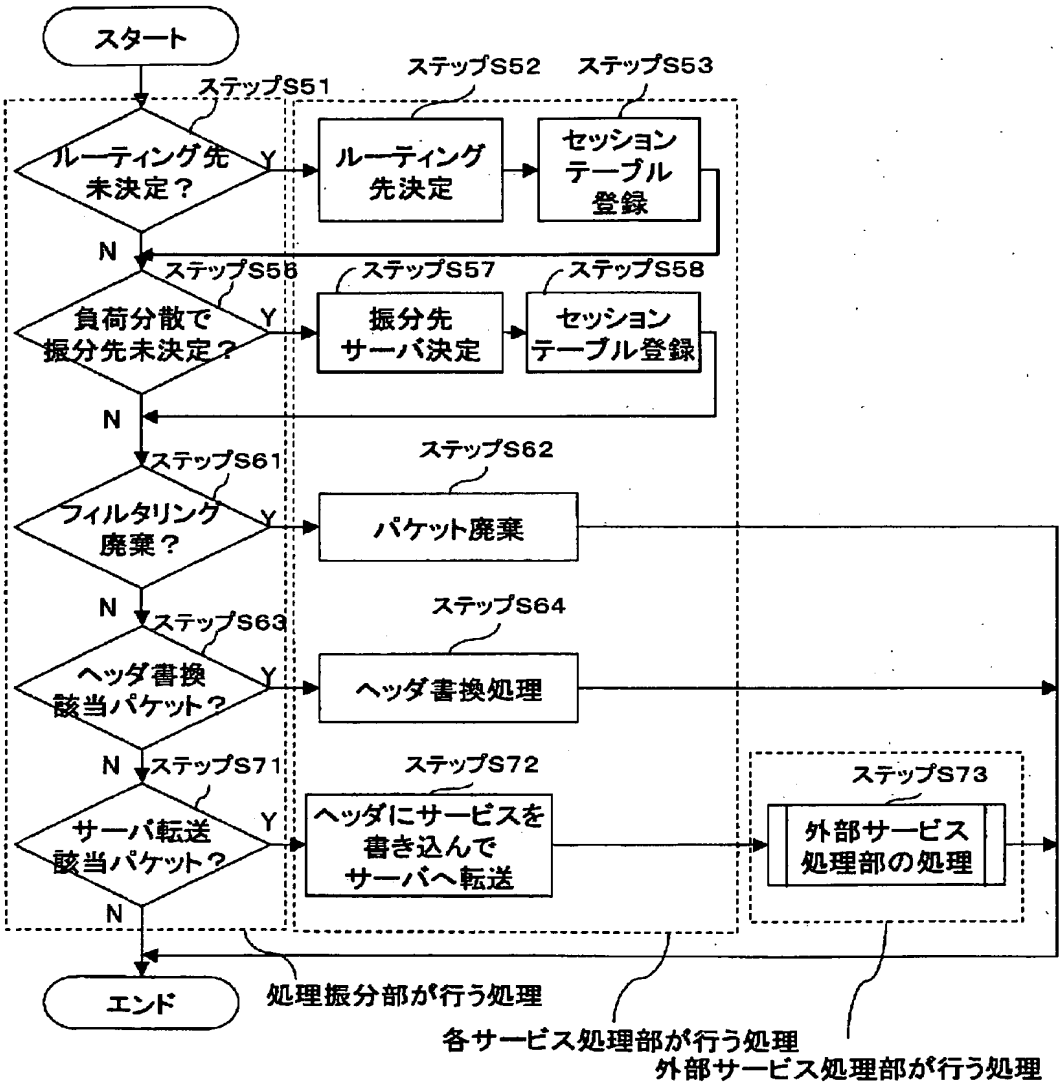
【図１８】

本発明の第4の実施例のパケット中継処理装置の構成を示す図



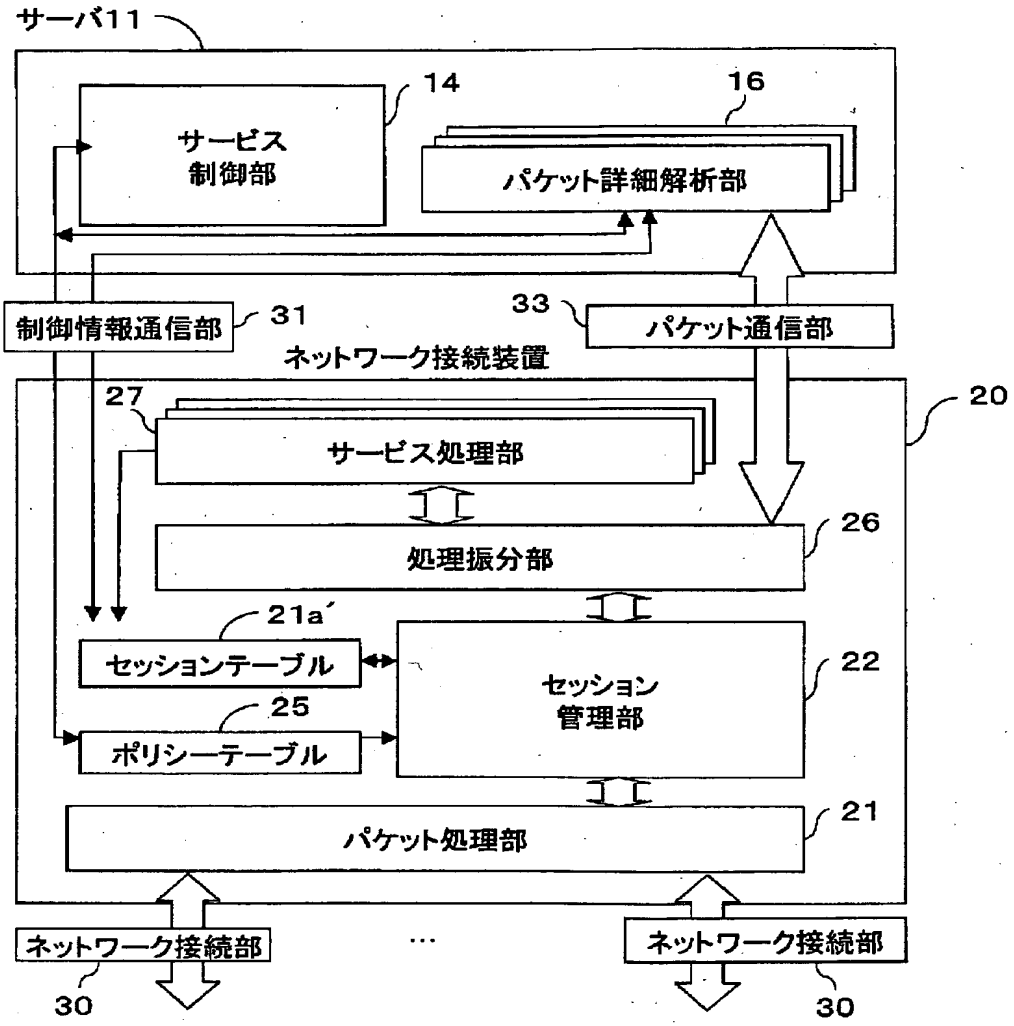
【図１９】

第4実施例に係る処理振分部、
サービス処理部及び外部サービス処理部における
処理の手順を示すフローチャート



【図２０】

本発明の第5の実施例のパケット中継処理装置の構成を示す図



【図２１】

第5実施例におけるセッションテーブルの一例を示す図（その1）

（URL 負荷分散、および URL フィルタリング）

セッションID		0	1	2	3	4	5
セッション検索キー	送信元IPアドレス	192.168.50.5	192.168.1.5	192.168.30.30	192.165.200.1	192.168.200.1	192.168.200.10
	送信元ポート番号	16321	8080	11950	http	3333	8080
	プロトコル	TCP	TCP	TCP	TCP	TCP	TCP
	宛先IPアドレス	192.168.1.5	192.168.50.5	192.168.200.1	192.168.30.30	192.168.200.10	192.168.200.1
	宛先ポート番号	8080	16321	http	11950	8080	3333
	入力インタフェース	0	1	0	Server	Server	1
セッション状態		IN SYN	IN SYN	ESTAB	ESTAB	IN SYN	IN SYN
出力元インタフェース		1	0	-	0	1	-
適用サービスタイプ		サーバ転送:ON URL フィルタリング	サーバ転送:ON URL フィルタリング	サーバ転送:ON URL 負荷分散	サーバ転送:ON URL 負荷分散	サーバ転送:ON URL 負荷分散	サーバ転送:ON URL 負荷分散
固有情報	変換用送信元IPアドレス	-	-	-	-	-	-
	変換用送信元ポート番号	-	-	-	-	-	-
	変換用宛先IPアドレス	-	-	-	-	-	-
	変換用宛先ポート番号	-	-	-	-	-	-
	シーケンス番号差分	-	-	-	-	-	-
	ACK番号差分	-	-	-	-	-	-
一貫性保持時間(ms)		1000	1000	3000	3000	3000	3000
イベントフラグ(パケット)		OFF	OFF	OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)		OFF	OFF	OFF	OFF	OFF	OFF

URL負荷分散

【図２２】

第5実施例におけるセッションテーブルの一例を示す図(その2)

(FTP フィルタリング)

セッションＩＤ		6	7
セッション検索キー	送信元ＩＰアドレス	192.168.2.100	192.168.25.250
	送信元ポート番号	3001	21
	プロトコル	TCP	TCP
	宛先ＩＰアドレス	192.168.25.250	192.168.2.100
	宛先ポート番号	21	3001
	入力インタフェース	0	1
セッション状態		IN SYN	IN SYN
出力先インタフェース		1	0
適用サービスタイプ		サーバ転送:ON FTP フィルタリング	サーバ転送:ON FTP フィルタリング
固有情報	変換用送信元ＩＰアドレス	-	-
	変換用送信元ポート番号	-	-
	変換用宛先ＩＰアドレス	-	-
	変換用宛先ポート番号	-	-
	シーケンス番号差分	-	-
	ＡＣＫ番号差分	-	-
属性保持時間(ms)		1000	1000
イベントフラグ(パケット)		OFF	OFF
イベントフラグ(ヘッダ)		OFF	OFF

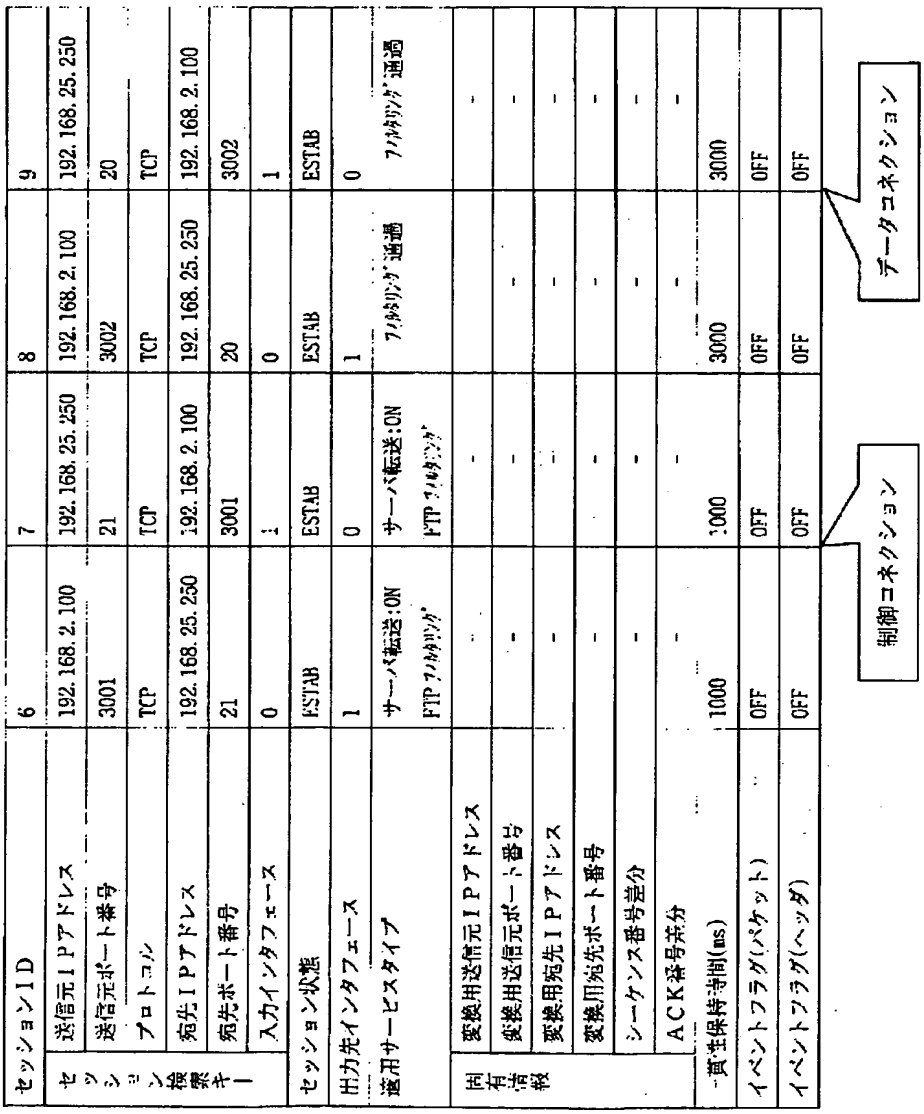
【図２３】

第5実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その1）（URL負荷分散、およびURLフィルタリング）

セッションID		0	1	2	5
セッション検索キー	送信元ＩＰアドレス	192.168.50.5	192.168.1.5	192.168.30.30	192.168.200.10
	送信元ポート番号	16321	8080	11950	8080
	プロトコル	TCP	TCP	TCP	TCP
	宛先ＩＰアドレス	192.168.1.5	192.168.50.5	192.168.200.1	192.168.200.1
	宛先ポート番号	8080	16321	http	3333
	入力インタフェース	0	1	0	1
セッション状態		ESTAB	ESTAB	ESTAB	ESTA3
出力先インタフェース		1	0	1	0
適用サービスタイプ		サーバ転送:OFF フィルタリング:通過	サーバ転送:OFF フィルタリング:通過	サーバ転送:OFF ヘッダ書換	サーバ転送:OFF ヘッダ書換
固有情報	変換用送信元ＩＰアドレス	-	-	192.168.200.1	
	変換用送信元ポート番号	-	-	http	
	変換用宛先ＩＰアドレス	-	-	192.168.200.10	192.168.30.30
	変換用宛先ポート番号	-	-	8080	11950
	シーケンス番号差分	-	-	2394	14733
	ＡＣＫ番号差分		-	54654	8002
資性保持時間(ms)		1000	1000	3000	3000
イベントフラグ(パケット)		OFF	OFF	OFF	OFF
イベントフラグ(ヘッダ)		OFF	OFF	OFF	OFF

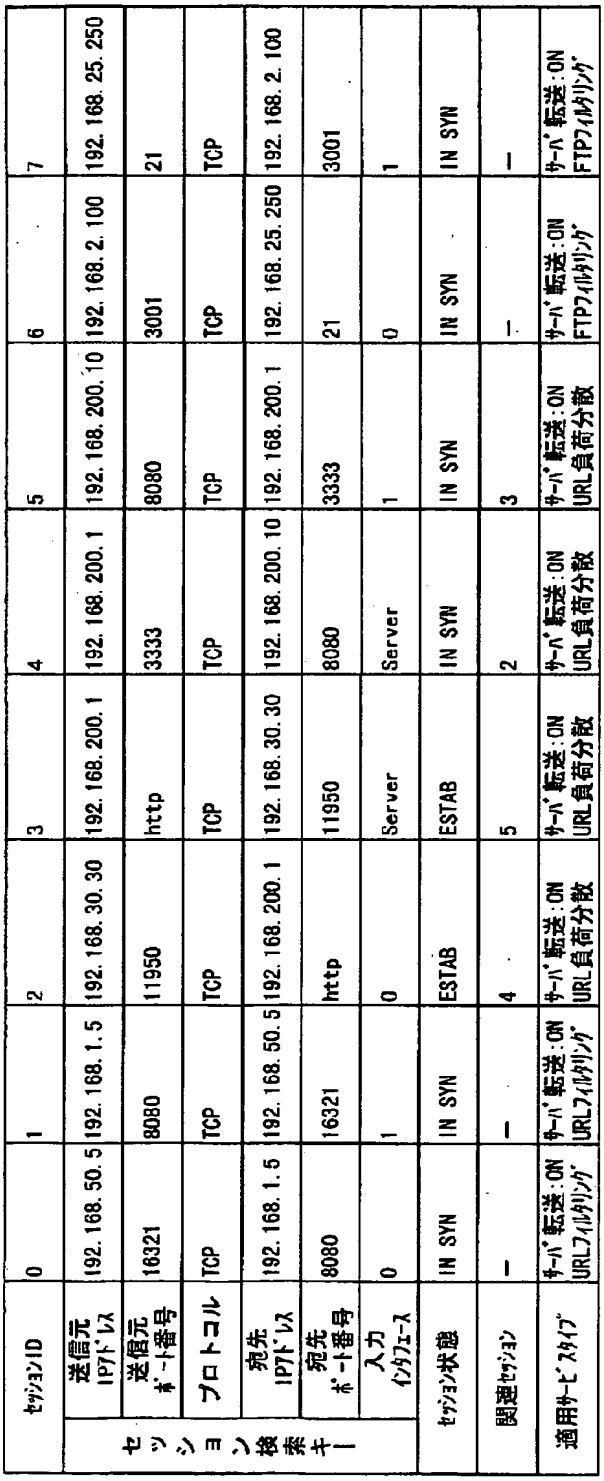
【図２４】

第5実施例におけるパケット詳細解析終了後のセッションテーブルの一例を示す図（その2）（FTPフィルタリング）



【図２５】

詳細解析用セッションテーブルの構成例を示す図



セッションID		0	1	2	3	4	5	6	7
セッション検索キー	送信元IPｱﾄﾞﾚｽ	192.168.50.5	192.168.1.5	192.168.30.30	192.168.200.1	192.168.200.1	192.168.200.10	192.168.2.100	192.168.25.250
	送信元ﾎﾟｰﾄ番号	16321	8080	11950	http	3333	8080	3001	21
	プロトコル	TCP	TCP	TCP	TCP	TCP	TCP	TCP	TCP
	宛先IPｱﾄﾞﾚｽ	192.168.1.5	192.168.50.5	192.168.200.1	192.168.30.30	192.168.200.10	192.168.200.1	192.168.25.250	192.168.2.100
	宛先ﾎﾟｰﾄ番号	8080	16321	http	11950	8080	3333	21	3001
	入力ｲﾝﾀﾌｪｰｽ	0	1	0	Server	Server	1	0	1
セッション状態		IN SYN	IN SYN	ESTAB	ESTAB	IN SYN	IN SYN	IN SYN	IN SYN
関連セッション		—	—	4	5	2	3	—	—
適用サービスタイプ		ｻｰﾊﾞ転送:ON URLﾌｨﾙﾀﾘﾝｸﾞ	ｻｰﾊﾞ転送:ON URLﾌｨﾙﾀﾘﾝｸﾞ	ｻｰﾊﾞ転送:ON URL負荷分散	ｻｰﾊﾞ転送:ON URL負荷分散	ｻｰﾊﾞ転送:ON URL負荷分散	ｻｰﾊﾞ転送:ON URL負荷分散	ｻｰﾊﾞ転送:ON FTPﾌｨﾙﾀﾘﾝｸﾞ	ｻｰﾊﾞ転送:ON FTPﾌｨﾙﾀﾘﾝｸﾞ

出証特２００１－３０９３３７２

【図２６】

詳細解析用ポリシーテーブルの構成例を示す図

URL フィルタリング用 URL テーブル

URL	通過/廃棄
www.xxx.com	廃棄
www2.yyy.co.jp	廃棄
bbb.ne.jp/~abc	廃棄
aaa.bbb.or.jp	廃棄

FTP フィルタリング用テーブル

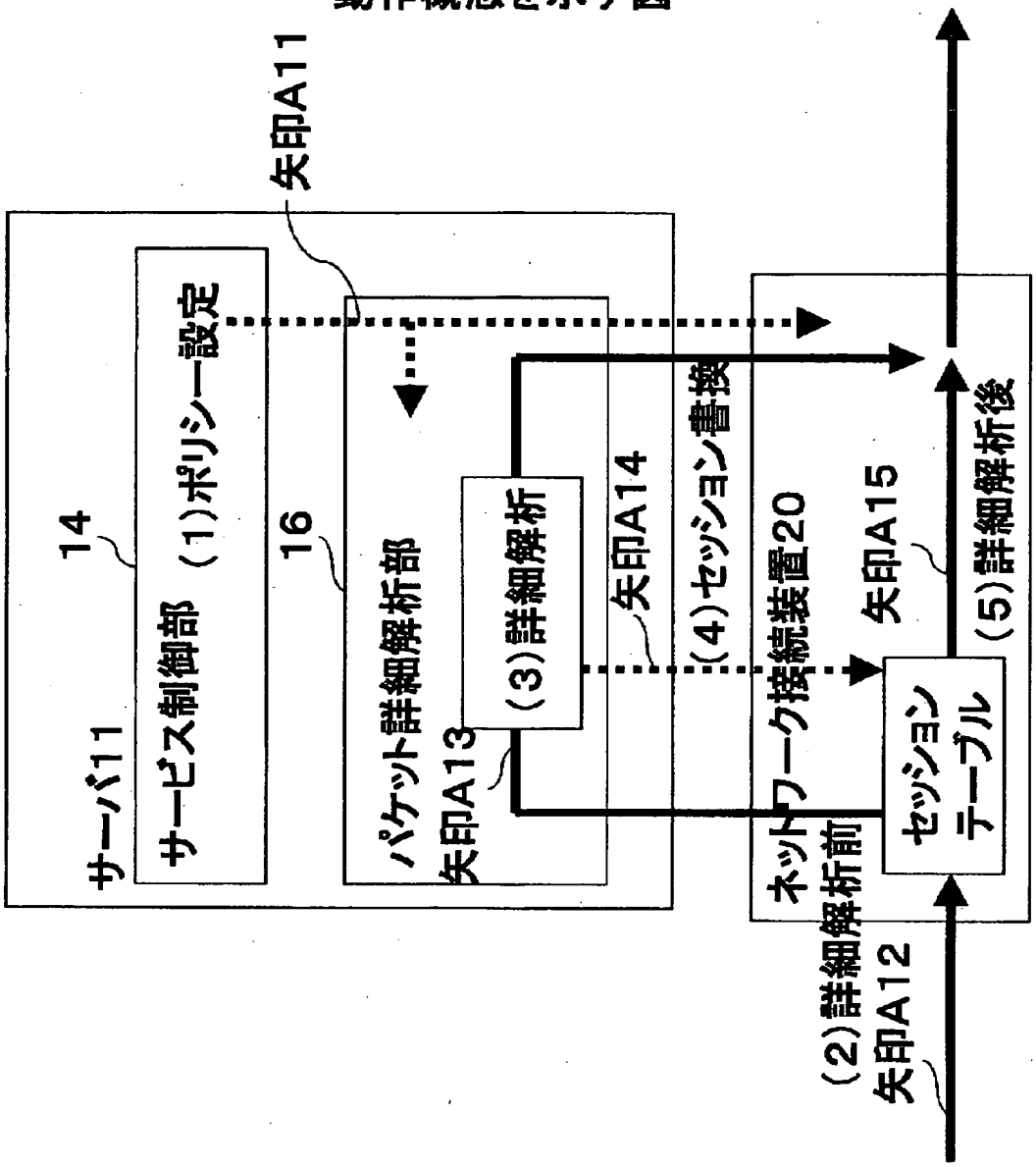
IP アドレス:ポート番号	通過/廃棄
192.168.1.5:Any	通過
192.168.2.100:Any	通過
192.168.150.*:Any	通過
192.168.250.*:Any	通過

URL 負荷分散用テーブル

URL	振分先
www.aaa.com	振分先 1: 192.168.200.10 振分先 2: 192.168.200.11 振分先 3: 192.168.200.12 振分先 4: 192.168.200.13 振分方法: ラウンドロビン
www.bbb.co.jp	振分先 1: 192.168.200.20 振分先 2: 192.168.200.21 振分先 3: 192.168.200.22 振分方法: ラウンドロビン
www.ccc.ne.jp	振分先 1: 192.168.200.30 振分先 2: 192.168.200.31 振分方法: ラウンドロビン
www.ddd.ne.jp/~abc	振分先 1: 192.168.200.40 振分先 2: 192.168.200.41 振分先 3: 192.168.200.42 振分先 4: 192.168.200.43 振分方法: ラウンドロビン

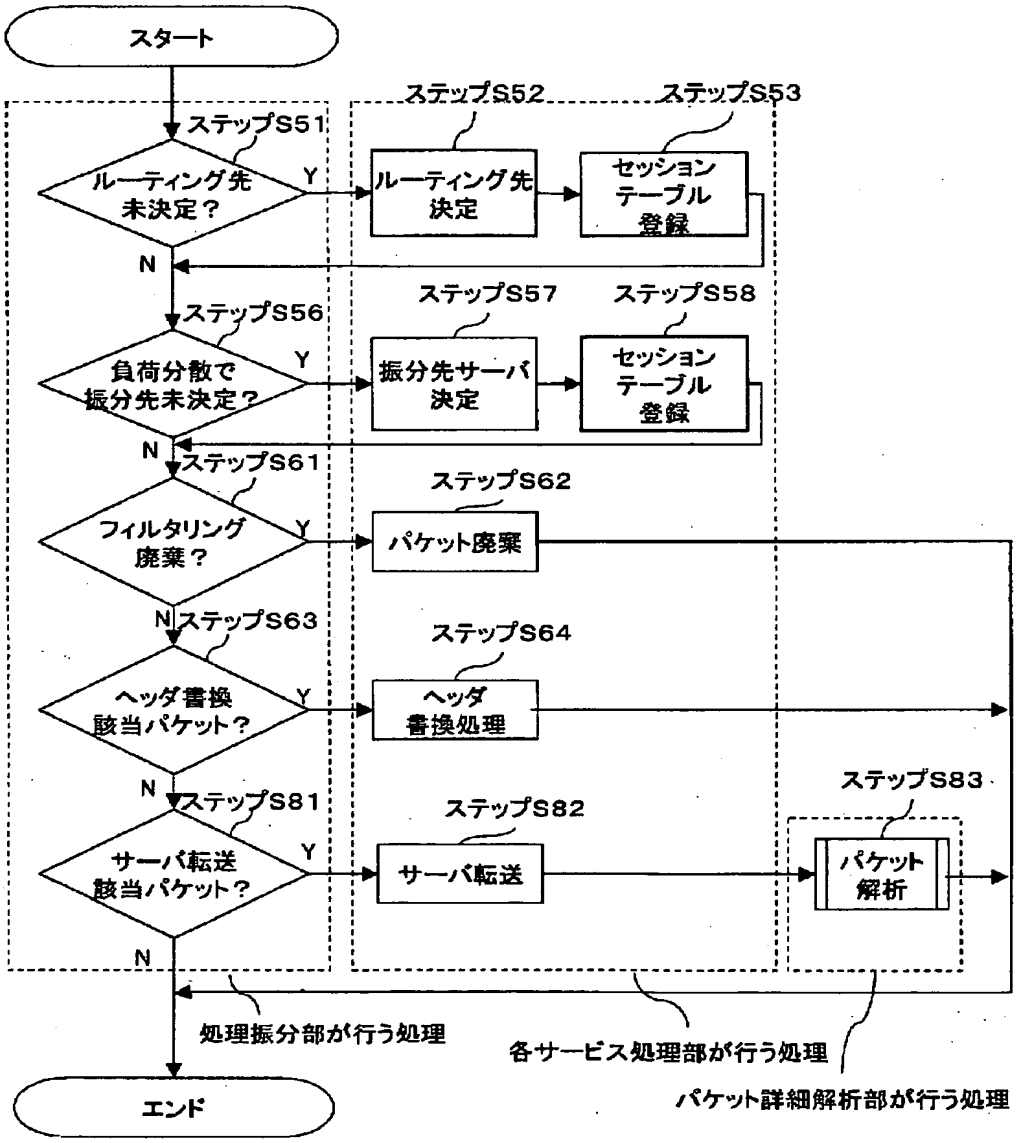
【図２７】

第5実施例に係るパケット中継処理装置の
動作概念を示す図



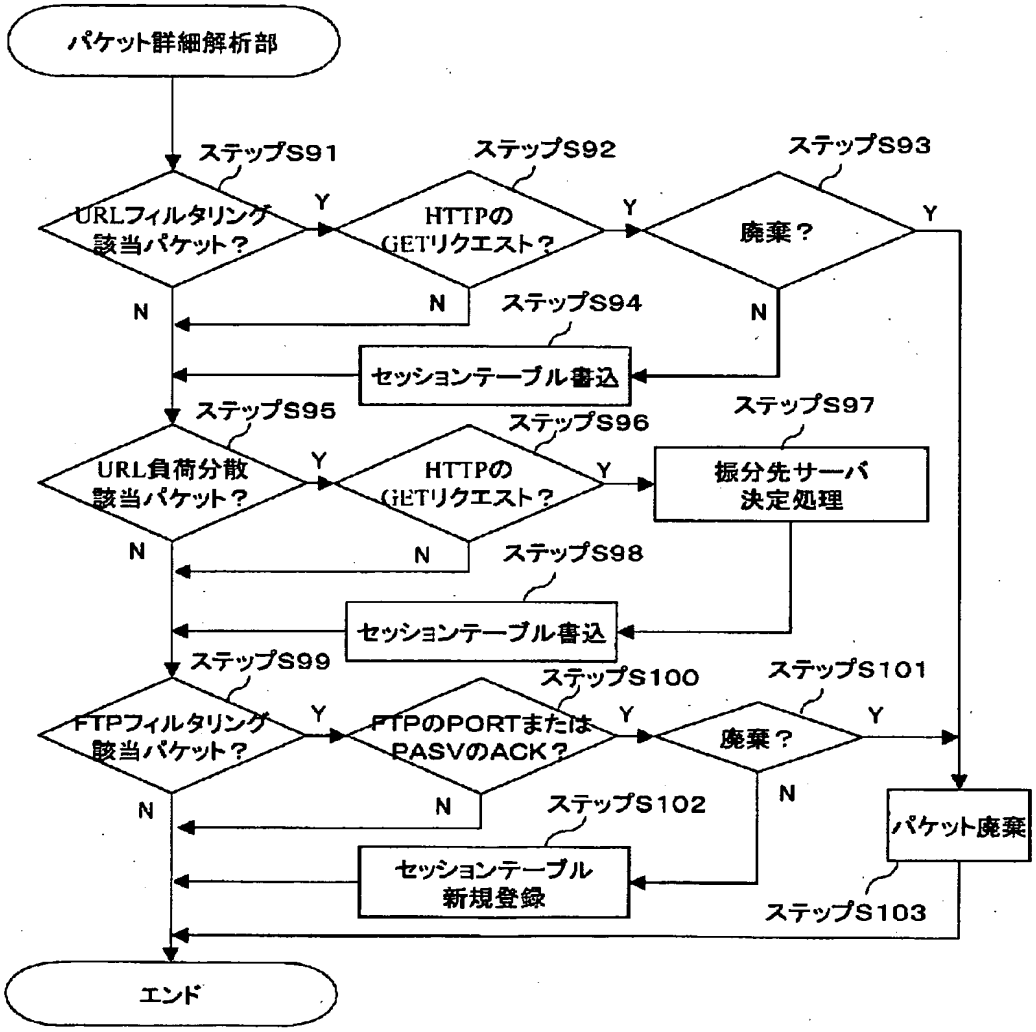
【図２８】

第5実施例に係る処理振分部、サービス処理部及び
パケット詳細解析部における処理の手順を示すフローチャート



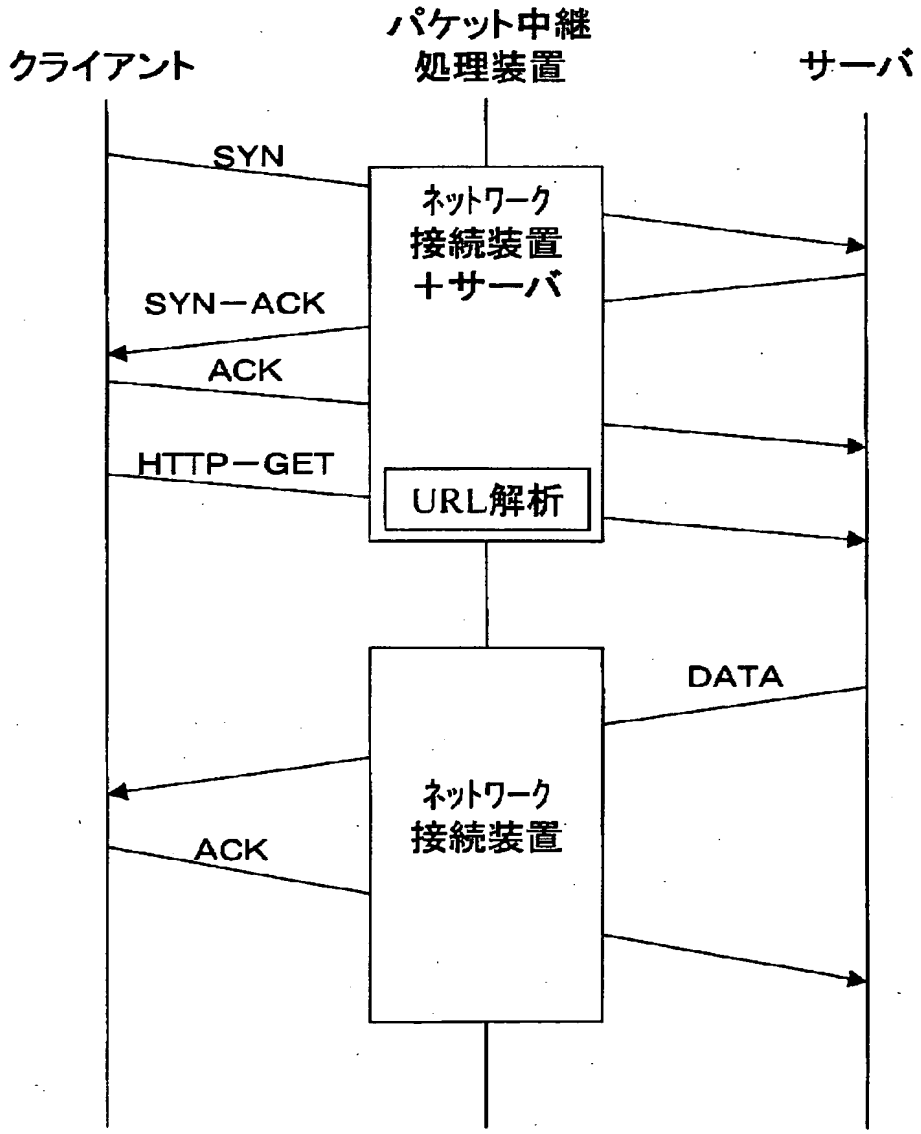
【図２９】

パケットの詳細解析における処理の手順を示すフローチャート



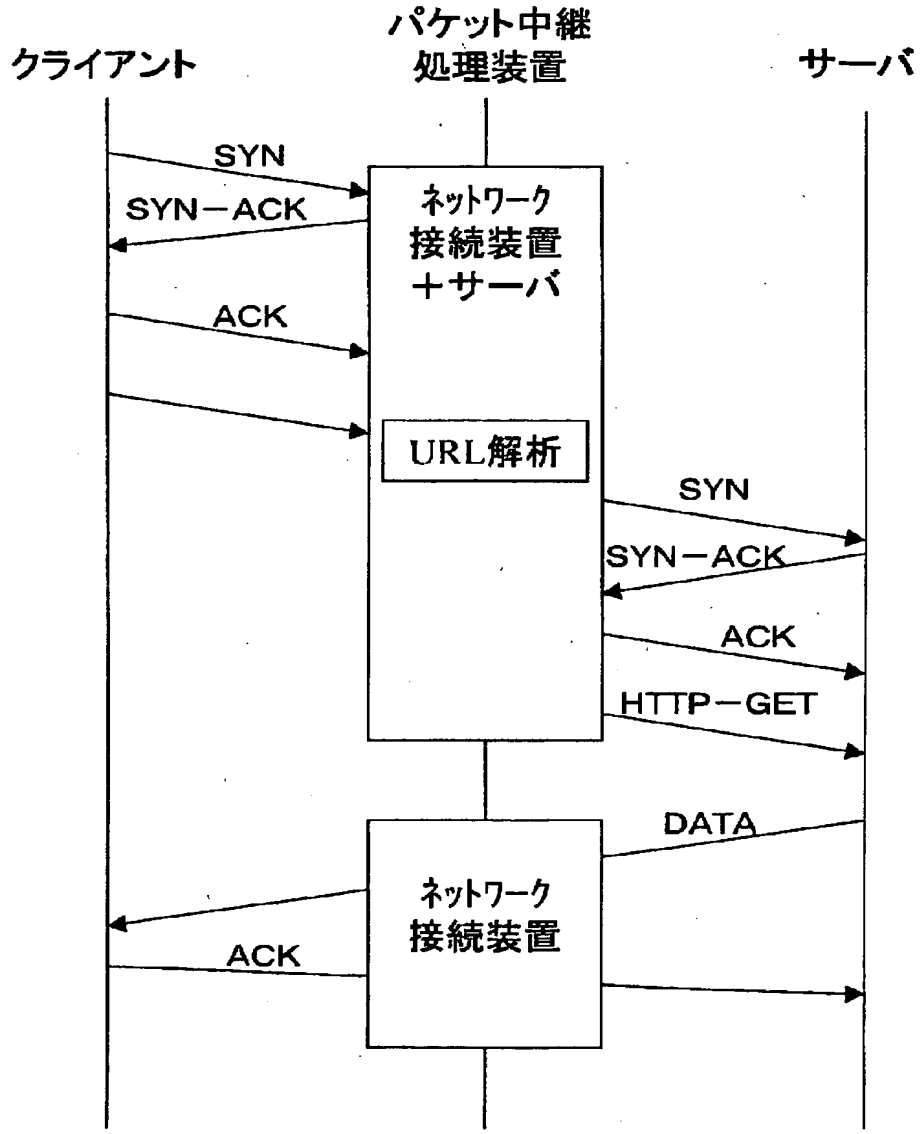
【図３０】

URLフィルタリングの動作を説明する図



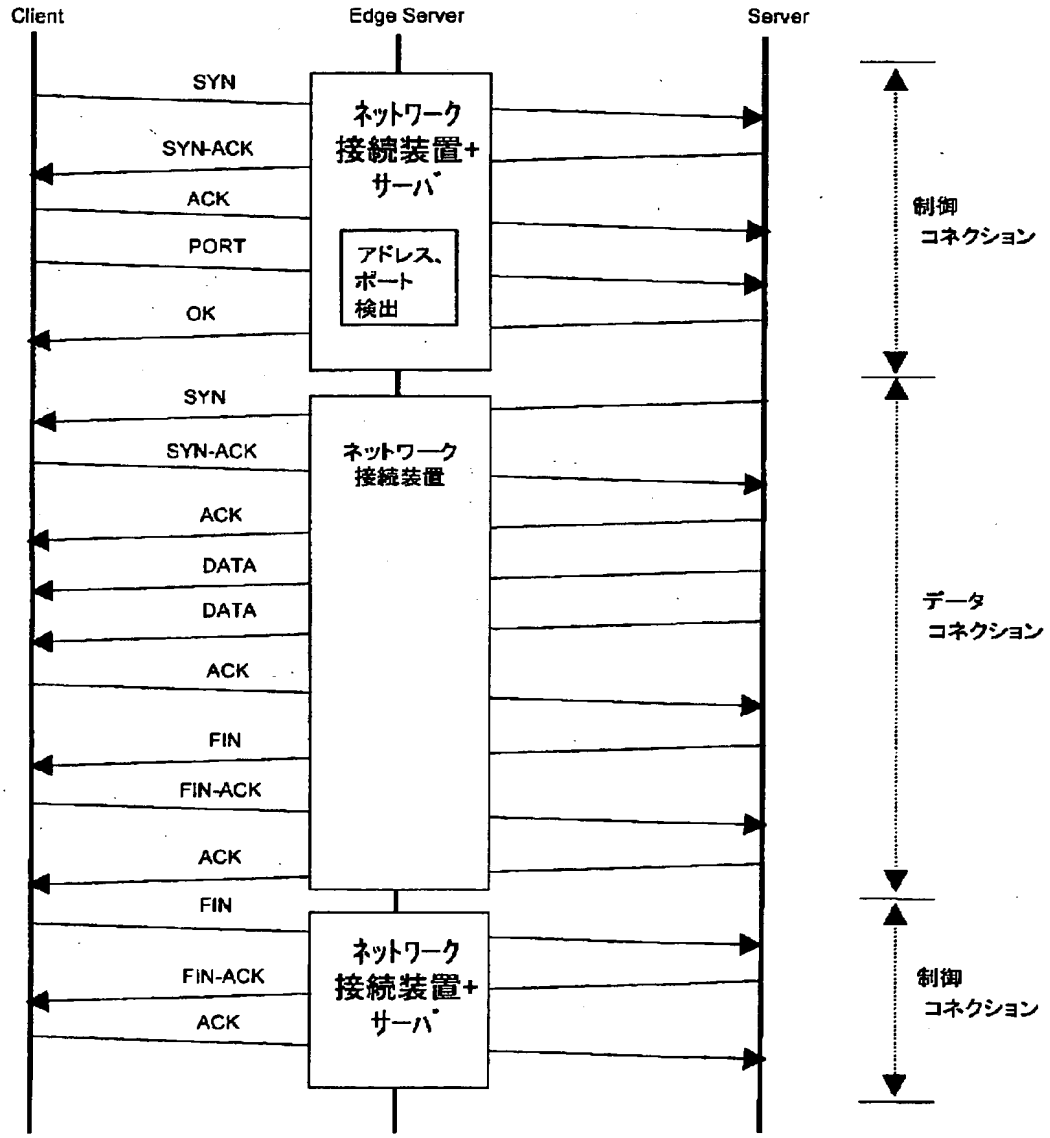
【図３１】

URL負荷分散の動作を説明する図



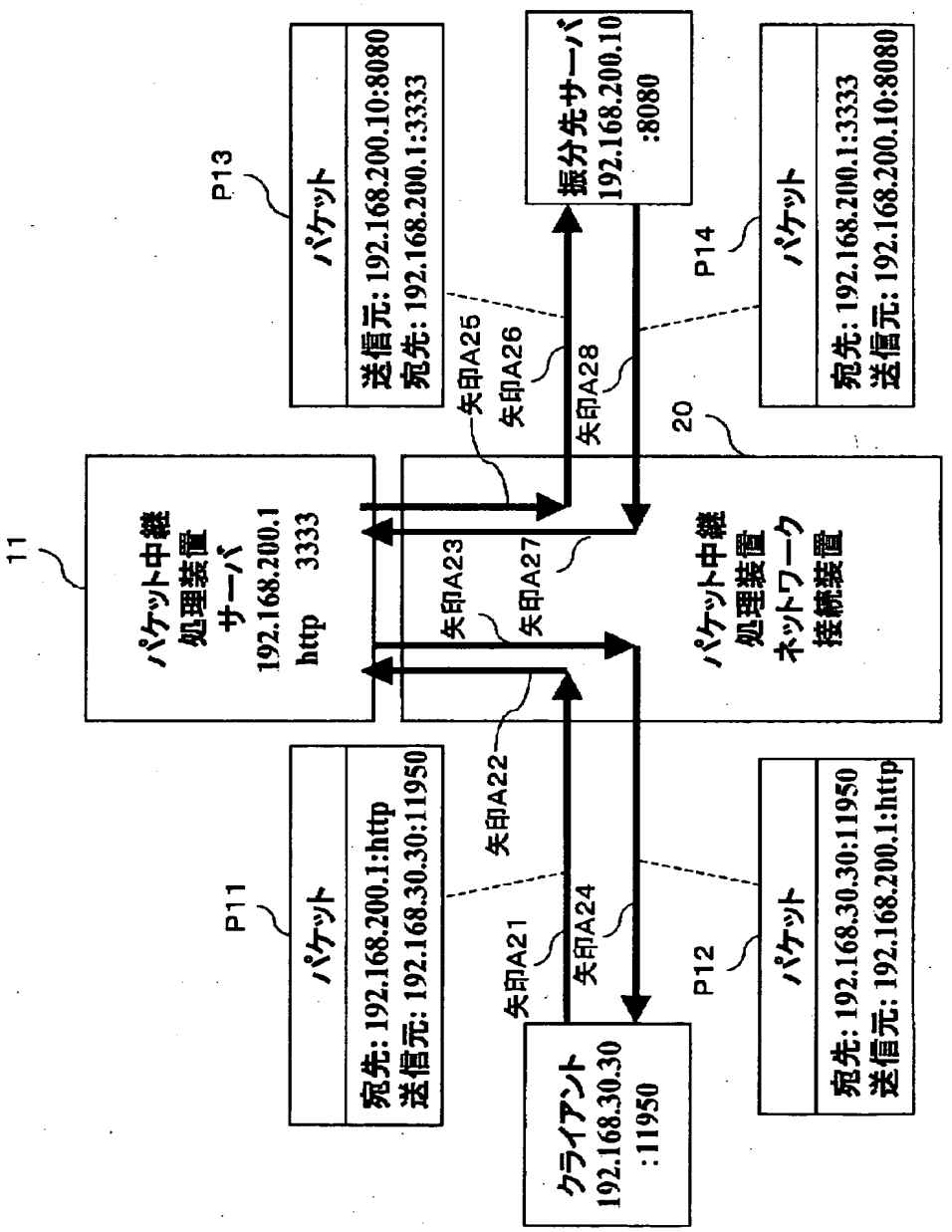
【図３２】

FTPフィルタリングの動作を説明する図



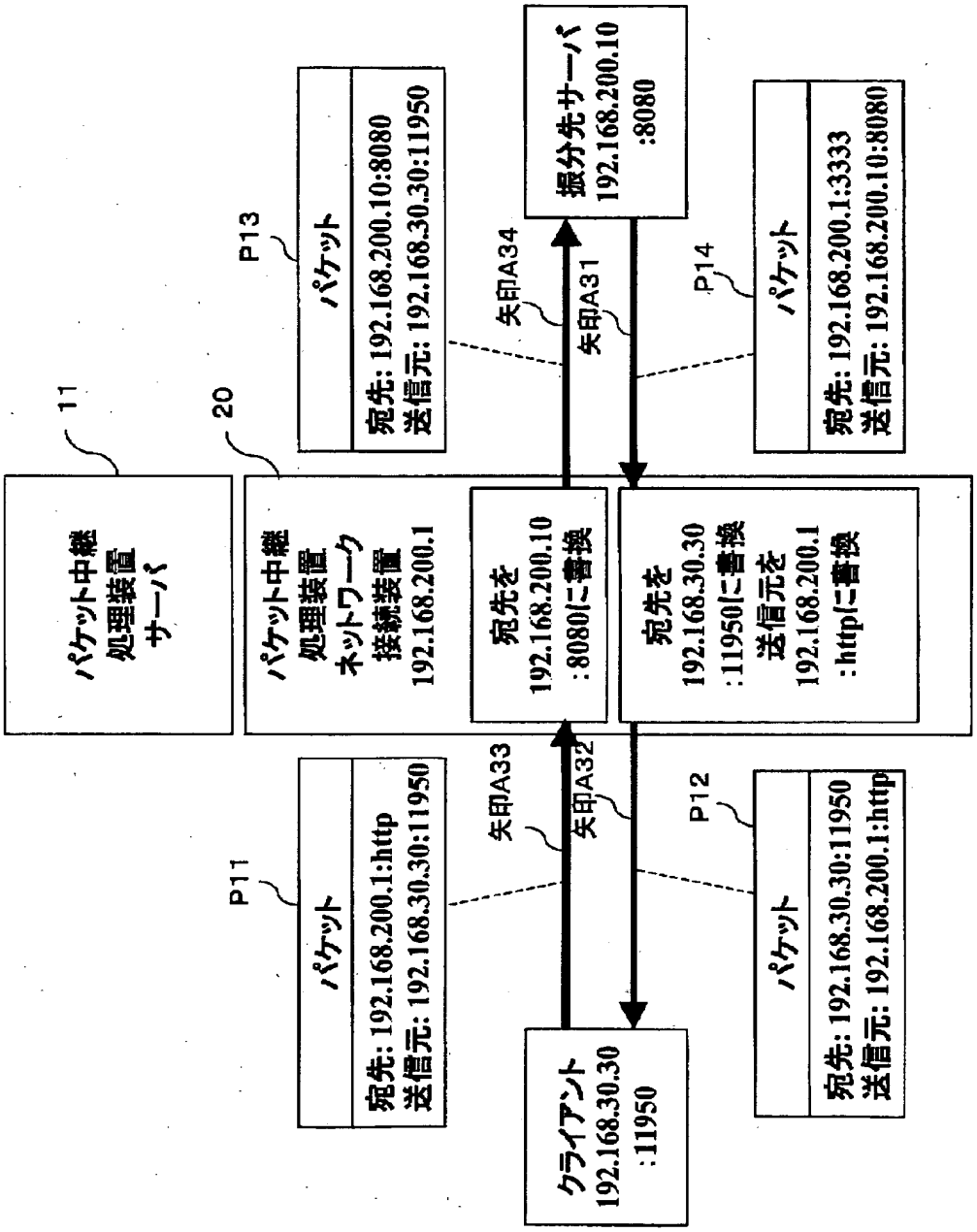
【図３３】

第5実施例におけるURL負荷分散サービスの
パケットフローを示す図（詳細解析前）



【図３４】

第5実施例におけるURL負荷分散サービスのパケットフローを示す図（詳細解析後）



【図３５】

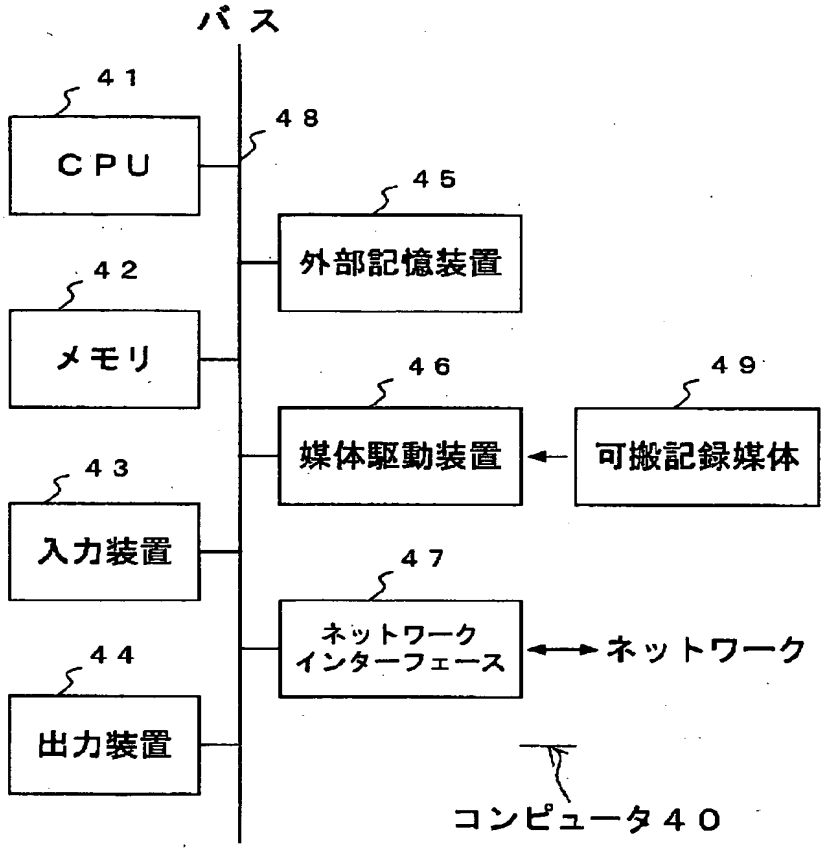
フラグテーブルのデータ構造の一例を示す図

グループＩＤ	フラグ
0	0
1	0
2	1
・ ・ ・	・ ・ ・
２５５	0

１：有効，０：無効

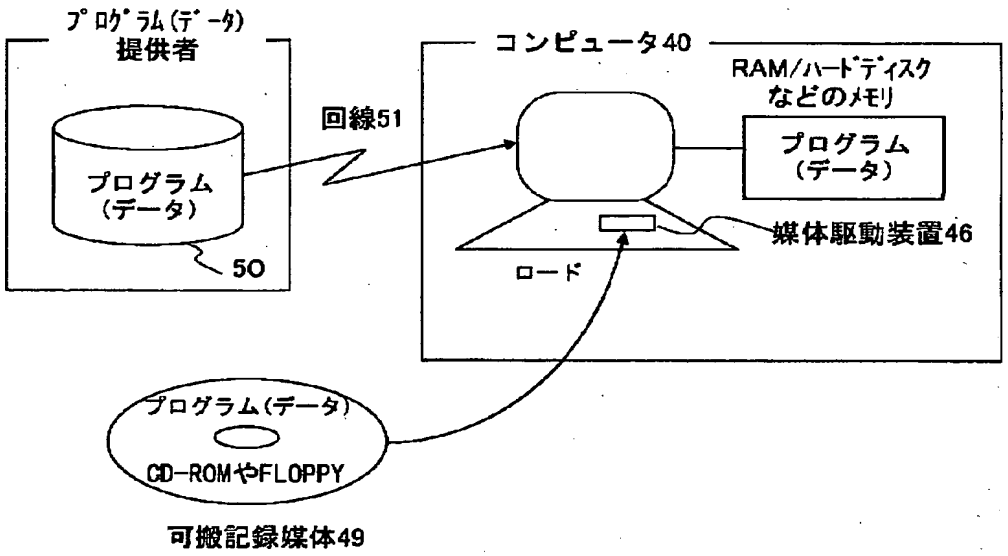
【図３６】

コンピュータの構成図



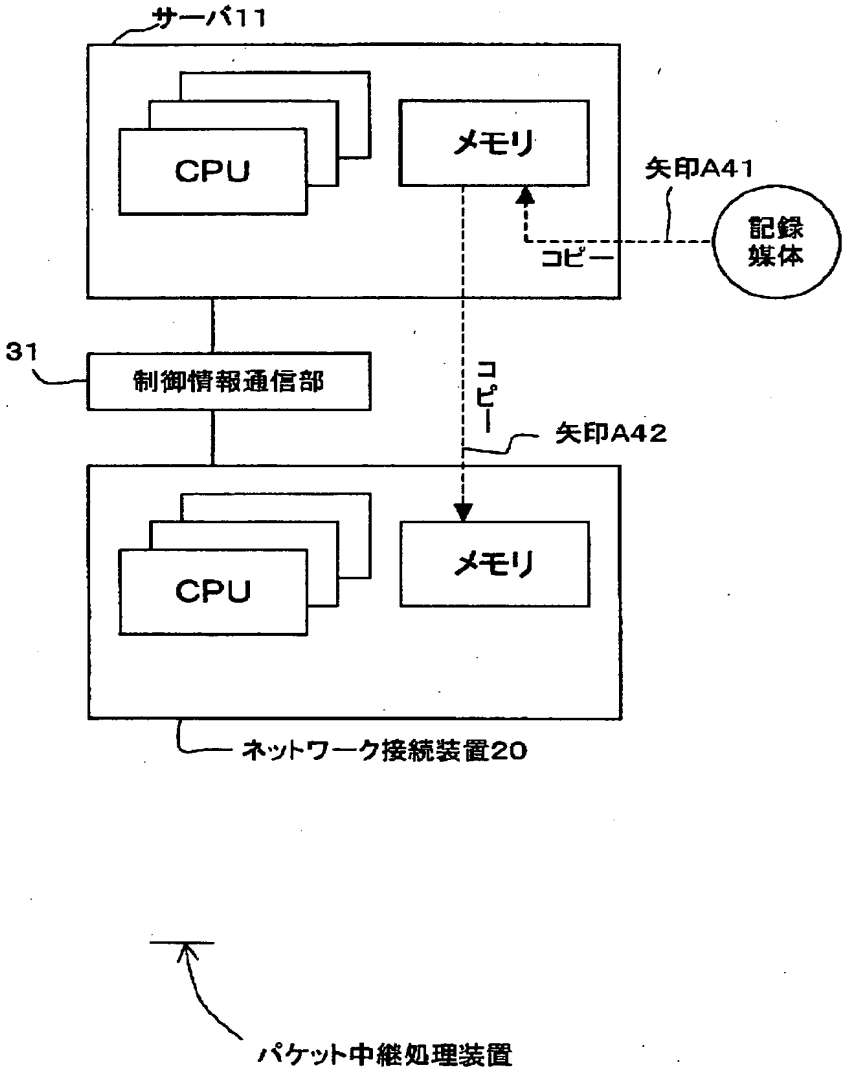
【図３７】

コンピュータにプログラムやデータを供給する
記録媒体や伝送記号を説明する図



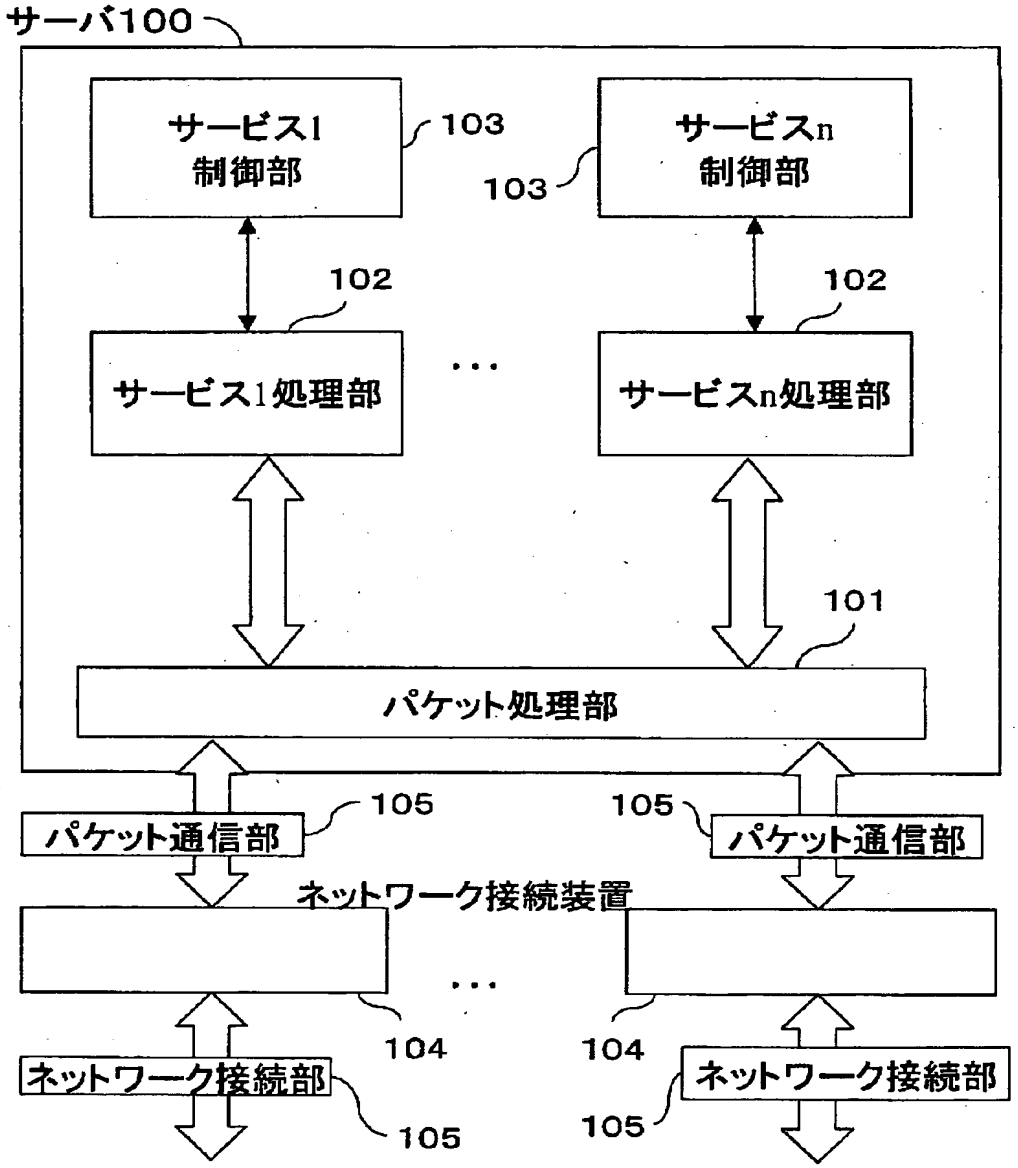
【図３８】

サーバ及びネットワーク接続装置へのプログラムやデータのローディングを説明する図



【図３９】

従来のパケット中継処理装置の構成を示す図



【書類名】　　要約書

【要約】

【課題】　多くのネットワークサービスで使用している共通処理を、ネットワーク接続装置に配置することにより、サーバのサービス処理を高速化すること。

【解決手段】　従来サーバ上に配置していたパケット処理部とセッション管理部をネットワーク接続装置２上に配置し、ネットワーク接続装置２上でセッション管理に基づくパケット中継処理を行う。また、ネットワーク装置２上に、処理振分部２ｃとサービス処理部２ｄを設け、サーバ１により設定されるポリシーに従って、処理振分部２ｃによりサービス処理部２ｄへのセッション管理に基づく振り分けを行う。さらに、条件に応じてサーバ１でセッション管理を行ったり、サーバにもサービス処理を行わせるようにしたり、サーバでパケットを解析してサービス内容を設定し、ネットワーク接続装置が、以後同じセッションに対して上記サービス内容に基づき中継処理を行うようにすることもできる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５２２３〕

１．変更年月日　　１９９６年　３月２６日
　［変更理由］　　住所変更
　　住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
　　氏　名　　富士通株式会社